Interoperability Test Specification

Mobile IPv6 /w IKEv1
Experimental version

Technical Document

Version 1.0.2

IPv6 Forum *http://www.ipv6forum.org*
IPv6 Ready Logo Committee *http://www.ipv6ready.org*

Modification Record

Version 1.0.2 July 23, 2007
Modify the copyright.

Version 1.0.1 July 24, 2006
Correction of cover and Acknowledgements.

Version 1.0.0 June 2, 2006
Experimental Version

Acknowledgement

IPv6 Forum would like to acknowledge the efforts of the following organizations in the development of this test specification.

- IPv6 Promotion Council
  Certification Working Group
  Mobile IPv6 Sub Working Group

- Commentators:
  IRISA-INRIA

Introduction

The IPv6 forum plays a major role to bring together industrial actors, to develop and deploy the next generation of IP protocols. Contrary to IPv4, which started with a small closed group of implementers, the universality of IPv6 leads to a huge number of implementations. Interoperability has always been considered as a critical feature in the Internet community. Due to the large number of IPv6 implementations, it is important to provide the market a strong signal proving the level of interoperability across various products. To avoid confusion in the mind of customers, a globally unique logo program should be defined. The IPv6 logo will give confidence to users that IPv6 is currently operational. It will also be a clear indication that the technology will still be used in the future. To summarize, this logo program will contribute to the feeling that IPv6 is available and ready to be used.

The IPv6 Logo Program consists of three phases:

Phase 1 :
In a first stage, the Logo will indicate that the product includes IPv6 mandatory core protocols and can interoperate with other IPv6 implementations.

Phase 2 :
The "IPv6 ready" step implies a proper care, technical consensus and clear technical references. The IPv6 ready logo will indicate that a product has successfully satisfied strong requirements stated by the IPv6 Logo Committee (v6LC).

To avoid confusion, the logo "IPv6 Ready" will be generic. The v6LC will define the test profiles with associated requirements for specific functionalities.

Phase 3 :
Same as Phase 2 with IPsec mandated.

This document is experimental version. This document includes an IKE function in addition to IPv6 Ready Logo Phase2 documents. "Mobile IPv6 w/ IKEv1" is experimental and IPv6 Ready Logo doesn't include IKE right now. However, we have sorted out the documents about IKE and we want to publish them here.

Table of Contents

[I] Interoperability Test Scenarios for Mobile IPv6

1. Overview

This document describes test scenarios to verify the interoperability between Mobile IPv6 equipment, in the form of Correspondent Nodes (CNs), Home Agents (HAs), and Mobile Nodes (MNs).

- Interoperability test scenario for IPv6 Ready Logo Phase 2 program

  "Interoperability test scenario for IPv6 Ready Logo Phase 2 program" includes all the test elements needed for acquisition of IPv6 Ready Logo Phase 2 program Logo. In particular, the test scenario covers all the Priority A1 and the Priority A2 defined in "IPv6 Ready Logo Phase 2 Policy" document. In this test scenario each Advanced Function can be selectively tested according to the implementation situation of Priority A2.

  Details of Priority A2 and the selection of the corresponding test elements in the test scenario are described in Section 2.

In following, Basic Functions are called "Priority A1" and Advanced Functions are called "Priority A2".

Acronyms

CN	- Correspondent Node
HA	- Home Agent
MN	- Mobile Node
FL	- Foreign Link
HL	- Home Link
HoA	- Home Address
CoA	- Care-of Address
BCE	- Binding Cache Entry
BLE	- Binding Update List Entry
BU	- Binding Update
BA	- Binding Acknowledgement
DHAAD	- Dynamic Home Agent Address Discovery
HAAD	- Home Agent Address Discovery

MPS	- Mobile Prefix Solicitation
MPA	- Mobile Prefix Advertisement
MPD	- Mobile Prefix Discovery
HoTI	- Home Test Init
HoT	- Home Test
CoTI	- Care-of Test Init
CoT	- Care-of Test
RR	- Return Routability
Co-Reg	- Correspondent Registration
De-Reg	- De-Registration
Re-Reg	- Re-Registration

Reference standards

This documentation covers the functions specified in the IETF RFC and Mobile IPv6 Test Profile listed below.

(1) RFC3775: Mobility Support in IPv6 (http://www.ietf.org/rfc/rfc3775.txt)

(2) RFC3776: Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents (http://www.ietf.org/rfc/rfc3776.txt)

(3) Guidelines for Implementation

(4) IPv6 Ready Logo Phase 2 Policy

2. Interoperability test scenario for IPv6 Ready Logo Phase 2 program

2.1 Phase 2 certification and support function

In order for Mobile IPv6 equipment (CN, HA, MN) to acquire Phase 2 Logo based on “IPv6 Ready Logo Phase 2 Policy”, all the Priority A1 must be supported in the viewpoint of interoperability. Furthermore, it is allowed that each Priority A2 can be selectively supported. In the case where Mobile IPv6 equipment with Priority A2 is certificated, the support status of Priority A2 should be clarified and tested properly.

The List of the Priority A1 and the Priority A2 defined in “IPv6 Ready Logo Phase 2 Policy” is shown in Table 2-1.

According to the support status of the Priority A2 shown in Table 2-1, the “Interoperability test scenario for IPv6 Ready Logo Phase 2 program” is to be configured as follows.

<1> Test elements for all the Priority A1 are included.

<2> Test elements for the Priority A2 should be executed selectively according to the support status of the target equipment.

Table 2-1. Priority A1 and Priority A2

Function	CN	HA	MN
Home Registration	-	A1	A1
BU/BA (IPsec ESP)	-	A1	A1
encapsulation/decapsulation	-	A1	A1
Movement detection	-	-	A1
CoA formation			
visiting of FL			
RR　(IPsec for HoTI/HoT)	A1	A2	A2
Co-Reg	A1	-	A2
Correspondent De-Reg	A1	-	A2

DHAAD	-	A2	A2
IKE without K bit**	-	A2	A2
IKE with K bit	-	A2	A2
MPD	-	A2	A2
Real HL	-	A2	A2
Mobile to Mobile*	-	-	A2

A1: Basic Function-Priority A1

A2: Advanced Function-Priority A2

The relationships between each Priority A1 / Priority A2 and the corresponding function item Number defined in "Guidelines for Implementation" are shown in Table 2-2.

* The precondition of Mobile to Mobile has the interoperability of CN function. If you apply for "Mobile to Mobile" function, you need to apply for "CN" function.

** IKEv1 is out of scope of requirements for "IPv6 Ready Logo Phase2 for MIPv6". However, the IKEv1 specification for MIPv6 is released as an experimental version.

Table 2-2. Requirements and References

Target	Function		Reference (Responding to Implementation Guideline)	
CN	Basic Function	RR	9.4.1	No. 1- 3
			9.4.2	No. 4- 6
			9.4.3	No. 7
			9.4.4	No. 8
		Co-Reg	9.1	No. 3- 7, 9- 10
			9.5.1	No. 1- 8, 11- 12, 19- 24
			9.5.2	No. 27- 28
			9.5.4	No. 35, 44, 47
		Correspondent De-Reg	9.5.3	No. 31- 33
			9.5.4	No. 45- 46
HA	Basic Function	Home Registration	10.1	No. 1, 3
			10.3.1	No. 1- 10, 18- 21, 23- 24, 26, 29- 30, 36- 38
		BU/BA (IPsec	4.1	No. 1, 3 - 4

		ESP)	4.2 No. 11- 13, 19- 20 4.3 No. 22- 24
		encapsulation/ decapsulatation	10.4.1 No. 1 10.4.2 No. 17- 20 10.4.5 No. 40, 42
	Advanced Function	IPsec for HoTI/HoT	10.4.2 No. 30 10.4.6 No. 44- 47 4.1 No. 5- 6 4.2 No. 14 4.3 No. 25- 28
		DHAAD	10.5.1 No. 1- 16
		IKE without K bit*	10.3.2 No. 44 4.1 No. 2 4.2 No. 21 4.4 No. 30- 31
		IKE with K bit*	Reference IKE without K bit 10.3.1 No. 27- 28 4.4 No. 32
		MPD	10.6.2 No. 2- 4, 8, 10- 13 10.6.3 No. 22- 28 4.1 No. 7- 8 4.2 No. 11- 13, 19 4.3 No. 22- 24
		Real HL	10.1 No. 2, 4, 6- 10 10.3.1 No. 13- 17 10.3.2 No. 40- 43, 45- 50 10.4.1 No. 2- 11, 13- 16 10.4.2 No. 22- 24 4.2 No. 16- 18
MN	Basic Function	Home Registration	11.1 No. 2- 5, 8- 10 11.7.1 No. 1- 8, 13, 18- 21 11.7.3 No. 54- 59, 61- 62
		BU/BA (IPsec ESP)	11.7.3 No. 51 4.1 No. 1, 3- 4

			4.2	No. 11- 13, 19
			4.3	No. 20- 22, 26, 32
		encapsulation / decapsulation	11.3.1	No. 4, 14- 16
		Movement detection, CoA formation, visiting of FL	11.5.1	No. 2, 4- 7
			11.5.2	No. 13
	Advanced Function	RR	11.1	No. 1- 16
			11.6.1	No. 1, 3- 8
			11.6.2	No. 10- 25
			11.6.3	No. 26- 27
			11.7.2	No. 27, 38, 40- 48
			11.7.3	No. 52- 59, 61- 63
			11.7.4	No. 71- 74
			4.1	No. 5- 6
			4.2	No. 14
			4.3	No. 23- 25, 27
			4.4	No. 32
		DHAAD	11.4.1	No. 1- 5, 7- 11
		IKE without K bit*	11.3.2	No. 28- 30
			11.7.1	No. 11- 12
			11.7.3	No. 65
			4.1	No. 2
			4.4	No. 28- 31
		IKE with K bit*	Reference IKE without K bit	
			11.7.3	No. 66
			4.4	No. 33
		MPD	11.4.2	No. 12- 26
			11.7.3	No. 60
			4.1	No. 7- 8
			4.2	No. 11- 13, 19
			4.3	No. 20- 22
			4.4	No. 32

		Real HL	11.3.1 No. 8 11.5.4 No. 32- 49 4.2 No. 16- 18
		Mobile to Mobile	Reference RR (CN) Reference Co-Reg (CN) Reference Correspondent De-Reg (CN) Reference RR (MN) 6.1 No. 1- 3

* IKEv1 is out of scope of requirements for “IPv6 Ready Logo Phase2 for MIPv6”. However, the IKEv1 specification for MIPv6 is released as an experimental version.

2.2 The architecture of the Interoperability test scenario

The Outline of the "Interoperability test scenario for IPv6 Ready Logo Phase 2 program" is the follows.

<1> First, one superset scenario, see table 2-3, that covers all the Priority A1 and all the Priority A2 is developed.

<2> Moreover, the scenario can be reconstructed by combining test elements of only Priority A2 that the target equipment supports.

<3> It is possible to verify the function of the preceding sequence by checking the proceeding sequence through the interoperability test scenarios.

<4> Intermediate checkpoints between major functions are set to confirm the progress of the testing.

Regarding the above point <1>, considering implementer's convenience and efficiency of the testing, the superset of the interoperability test scenarios that covers all the Priority A1 and Priority A2 is developed to execute all the required tests with a minimum process. This superset of the interoperability test scenarios can be built by combining every test element corresponding to each Functional Unit[1].

As for point <2> above, the Functional Units of Priority A2 that are not supported by the target Mobile IPv6 equipment (HA, and MN) can be skipped and only the Functional Units of the supported Priority A2 can be executed in the test scenario. This architecture enables the test scenario to be applied to various implementation situations. Examples are shown in Figures 2-1 and 2-2.

In "Interoperability test scenario for IPv6 Ready Logo Phase 2 program", the state of just before a Functional Unit (No. 1 A2-1, Figure 2-1) added to verify a Priority A2 (e.g. DHAAD) and the state immediately after it are the same, and the added Functional Unit (No. 1 A2-1, Figure 2-1) is smoothly connected with Functional Unit (No. 0 A1-1, Figure 2-1) before it and Functional Unit (No. 2 A1-1, Figure 2-1) just after it. Therefore, the "Interoperability test scenario for IPv6 Ready Logo Phase 2 program" has a construction by which an implementer

[1] Functional Unit: A minimum set of sequences and procedures needed for verifying a specific function included in "Interoperability test scenarios for IPv6 Ready Logo Phase 2 program."

can verify all Priority A1 and Priority A2 in an arbitrary combination.

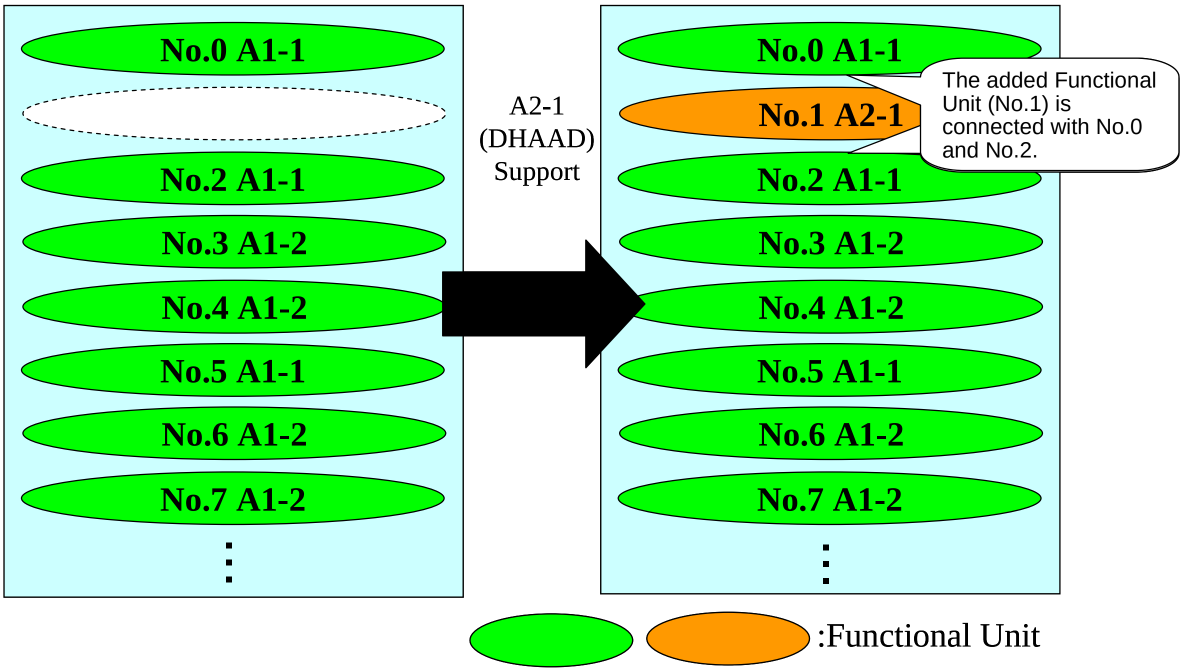


Figure 2-1. Scenario Architecture (1)

In point <3>, the "Interoperability test scenario for IPv6 Ready Logo Phase 2 program" consists of sequences of normal operation of Mobile IPv6 equipment (CN, HA, MN), and each Functional Unit in the interoperability test scenarios is executed not only for verifying its function, but for verifying the function of the Functional Unit before it. This architecture of interoperability test scenarios is explained in Figure 2-2 in more detail.
(Figure 2-2 corresponds from sequence No. 1 to No.8 of Section 3.3.)

For example, Functional Unit (No. 3 A1-1, Figure 2-2) is executed not only for verifying its function but also for verifying the function of Functional Unit (No. 1 A2-1, Figure 2-2) and Functional Unit (No. 2 A2-2, Figure 2-2). Therefore, checking that sequences in packet logs collected during the test are the same as sequences in "Interoperability test scenarios for IPv6 Ready Logo Phase 2 program" becomes the check of each function.

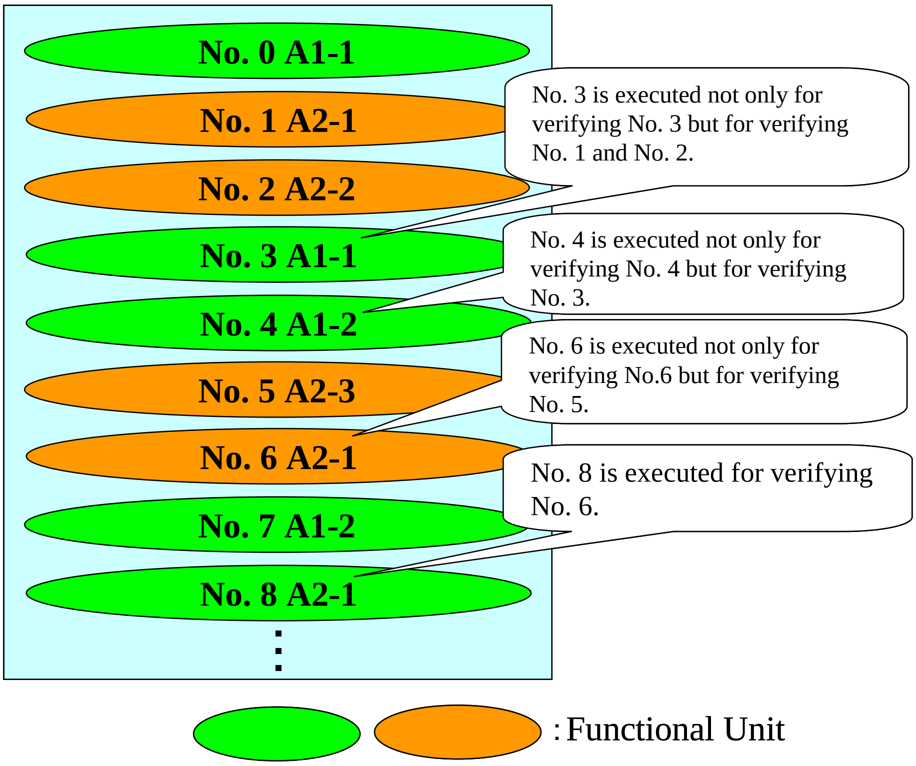

No. 0 A1-1
No. 1 A2-1
No. 2 A2-2
No. 3 A1-1
No. 4 A1-2
No. 5 A2-3
No. 6 A2-1
No. 7 A1-2
No. 8 A2-1
No. 3 is executed not only for verifying No. 3 but for verifying No. 1 and No. 2.
No. 4 is executed not only for verifying No. 4 but for verifying No. 3.
No. 6 is executed not only for verifying No.6 but for verifying No. 5.
No. 8 is executed for verifying No. 6.
: Functional Unit

Figure 2-2. Scenario Architecture (2)

In point <4>, the checkpoints which can be grouped as a Functional check unit are set in the interoperability test scenarios so that an implementer can verify the status of the test process. The contents of the check are described in the test procedure document (see Section 3). If the target Mobile IPv6 equipment (CN, HA and MN) has the function to display the state of the equipment, the function can be used with the methods in the test procedure document in order to execute tests more efficiently and accurately.

For example, in Table 2-3, verifying functions of the Functional Units from No. 0 to No. 8 is completed by Unit No. 8, and the Functional Units from No. 0 to No. 8 are grouped as a Functional check unit. Besides this example, there are some Functional Sets[2] grouped as a Functional check unit, and they are specified by thick lines in Table 2-3.

[2] Functional Set: The checkpoint which can be grouped as a Functional check unit in "Interoperability test scenarios for IPv6 Ready Logo Phase 2 program."

2.3 Interoperability test scenario for IPv6 Ready Logo Phase 2 program

The “Interoperability test scenario for IPv6 Ready Logo Phase 2 program” was developed from the viewpoint of the Phase 2 certification, as shown in Table 2-3. The selection method of the “Interoperability test scenario for IPv6 Ready Logo Phase 2 program” is explained by Table 2-3.

Since all the Priority A1 are indispensable for Mobile IPv6 equipment (CN, HA, and MN) to acquire a Phase 2 Logo, all the Functional Units for verifying Priority A1 (the column of Required Functions in Table 2-3 is "A1") must be included in the “Interoperability test scenario for IPv6 Ready Logo Phase 2 program”. When an MN or an HA is a candidate for Phase 2 certification, the Functional Units of No. 0, 3, 4, 7, 11, 12, 14, 17 and 19 in Table 2-3 must be included in the “Interoperability test scenario for IPv6 Ready Logo Phase 2 program”. When a CN is a candidate for Phase 2 certification, Functional Units of No. 0, 3, 4, 6, 7, 8, 11, 12, 13, 14, 15, 17, 18 and 19 in Table 2-3 must be included in the “Interoperability test scenario for IPv6 Ready Logo Phase 2 program”.

Furthermore, when an HA or an MN acquires a Phase 2 Logo on the condition of supporting only a Priority A2 represented by A2-a without supporting another Priority A2 represented by A2-b, the interoperability test scenarios, which include all Functional Units for verifying A2-a (the columns of Required Functions in Table 2-3 are "A1" or "A1 and A2-a"), are selected, and the interoperability test scenarios, which include Functional Units for verifying A2-b (the columns of Required Functions in Table 2-3 are "A1 and A2-b" or "A1, A2-a and A2-b"), are not selected.

Furthermore, when an HA or an MN acquires a Phase 2 Logo on the condition of supporting A2-a and A2-b, the interoperability test scenarios, which include all the Functional Units for verifying A2-a and A2-b (the columns of Required Functions in Table 2-3 are "A1" or "A1 and A2-a" or "A1 and A2-b" or "A1, A2-a and A2-b"), are selected.

The column of “Verify other functional unit” in Table 2-3 shows the numbers for Functional Units which can be checked by the result of proceeding Functional Unit.

CN0 is CN as a test object, HA0 or HA2 is HA as a test object, and MN0 or MN1 is MN as a test object.

Table 2-3. interoperability test scenario

Functional Set	No	Functional Unit	Required Functions					Verify other Functional Unit
			MN0	HA0	CN0	MN1	HA2	
Home Registra-tion from FL	0	Boot up MN under FL	A1		-			
	1	DHAAD	A1 and DHAAD	A1 and DHAAD	-			
	2	IKE phase 1 + phase 2 （BU/BA）	A1 and IKE	A1and IKE	-			
	3	BU/BA （Initial Registration）	A1		-			No. 1 and 2
	4	ICMP echo request (CN->MN)	A1		-			No 3
	5	IKE ph2 （HoTI/HoT）	A1, IKE and RR	A1, IKE and IPsec for HoTI/HoT	A1			
	6	RR and BU/BA (Co-Reg)	A1 and RR	A1 and IPsec for HoTI/HoT	A1			No 5
	7	ICMP echo reply (MN->CN)	A1		-			No 3 and 6
	8	ICMP echo request (CN->MN) ICMP echo reply (MN->CN)	A1 and RR	A1 and IPsec for HoTI/HoT	A1			No 6
Home Registration from FL with MPD	9	IKE phase2 (MPS/MPA)	A1, IKE and MPD	A1, IKE and MPD	-			
	10	MPS/MPA	A1 and MPD	A1 and MPD	-			No 9
Home Re-Registration	11	BU/BA （Re-Reg）	A1		-			
	12	ICMP echo request (CN->MN)	A1		-			

from FL	13	RR and BU/BA (Co-Reg)	A1 and RR	A1 and IPsec for HoTI/HoT	A1			
	14	ICMP echo reply (MN->CN)	A1		-			No.11
	15	ICMP echo request (CN->MN) ICMP echo reply (MN->CN)	A1 and RR	A1 and IPsec for HoTI/HoT	A1			No.13
Moving from FL to FL’	16	IKE phase 2（BU/BA) (Re-keying)	A1 and IKE	A1 and IKE	-			
	17	BU/BA （Moving)	A1		-			No.16
	18	RR and BU/BA (Co-Reg)	A1 and RR	A1 and IPsec for HoTI/HoT	A1			
	19	ICMP echo request (CN->MN) ICMP echo reply (MN->CN)	A1		-			No. 17 and 18
Moving from FL’ to FL	20	IKE phase 2 （BU/BA) (Re-keying) or	A1 and IKE with K bit ->IKE phase 2	A1 and IKE with K bit ->IKE phase 2	-			
		IKE phase1and phase 2 （BU/BA）(Re-keying)	A1 and IKE without K bit ->IKE phase 1 and phase 2	A1 and IKE without K bit ->IKE phase 1 and phase 2				
	21	BU/BA（Moving)	A1 and IKE	A1 and IKE	-			No. 20
	22	ICMP echo request (CN->MN)	A1 and IKE	A1 and IKE	-			
	23	RR and BU/BA (Co-Reg)	A1, IKE and RR	A1, IKE and IPsec for HoTI/HoT	A1			

	24	ICMP echo reply (MN->CN)	A1 and IKE	A1 and IKE	-			No. 21
	25	ICMP echo request (CN->MN) ICMP echo reply (MN->CN)	A1, IKE and RR	A1, IKE and IPsec for HoTI/HoT	A1			No. 23
Returning Home	26	BU/BA　（Moving and De-Reg）	A1 and Real HL	A1 and Real HL	-			
	27	RR+BU/BA (De-Reg)	A1, Real HL and RR	A1, Returning Home and RR	A1			
	28	ICMP echo request (CN->MN) ICMP echo reply (MN->CN)	A1 and Real HL	A1 and Real HL	-			No. 26 and 27
Bootup under HL	29	Shutdown MN under HL	A1 and Real HL	A1and Real HL	-			
	30	Boot up MN under HL	A1 and Real HL	A1and Real HL	-			
	31	ICMP echo request (CN->MN) ICMP echo reply (MN->CN)	A1 and Real HL	A1 and Real HL	-			No. 30
Moving from HL to FL	32	Moving	A1 and Real HL	A1 and Real HL	-			
	33	DHAAD	A1, Real HL and DHAAD	A1, Real HL and DHAAD	-			
	34	IKE phase 1 and phase 2（BU/BA）	A1, Real HL and IKE	A1, Real HL and IKE	-			
	35	BU/BA　（Moving）	A1 and Real HL	A1 and Real HL	-			No. 33 and 34
	36	ICMP echo request (CN->MN)	A1 and Real HL	A1 and Real HL	-			
	37	IKE phase2 （HoTI/HoT）	A1, Real HL , IKE and RR	A1, Real HL, IKE and IPsec for HoTI/HoT	A1			

	38	RR and BU/BA (Co-Reg)	A1, Real HL and RR	A1, Real HL and IPsec for HoTI/HoT	A1			No. 37
	39	ICMP echo reply (MN->CN)	A1 and Real HL	A1 and Real HL	-			No. 35
	40	ICMP echo request (CN->MN) ICMP echo reply (MN->CN)	A1, Real HL and RR	A1, Real HL and IPsec for HoTI/HoT	A1			No. 38
Mobile to Mobile	41	Boot up another MN under FL	A1 and Mobile to Mobile	A1 and IPsec for HoTI/HoT		A1 and Mobile to Mobile	A1 and IPsec for HoTI/HoT	
	42	DHAAD （MN1<->HA2）	A1, Mobile to Mobile and DHAAD	A1, IPsec for HoTI/HoT and DHAAD		A1, Mobile to Mobile and DHAAD	A1, IPsec for HoTI/HoT and DHAAD	
	43	IKE phase 1 and phase 2（BU/BA）	A1, Mobile to Mobile and IKE	A1, IPsec for HoTI/HoT and IKE		A1, Mobile to Mobile and IKE	A1, IPsec for HoTI/HoT and IKE	
	44	BU/BA（Initial Registration, MN1<->HA2）	A1 and Mobile to Mobile	A1 and IPsec for HoTI/HoT		A1 and Mobile to Mobile	A1 and IPsec for HoTI/HoT	
	45	IKE phase2 （HoTI/HoT, MN1<->HA2）	A1, Mobile to Mobile and IKE	A1, IPsec for HoTI/HoT and IKE		A1, Mobile to Mobile and IKE	A1, IPsec for HoTI/HoT and IKE	
	46	ICMP echo request (MN1->MN0)	A1 and Mobile to Mobile	A1 and IPsec for HoTI/HoT		A1 and Mobile to Mobile	A1 and IPsec for HoTI/HoT	
	47	RR and BU/BA (Co-Reg, MN0->MN1)	A1 and Mobile to Mobile	A1 and IPsec for HoTI/HoT		A1 and Mobile to Mobile	A1 and IPsec for HoTI/HoT	
	48	ICMP echo reply (MN1->MN0)	A1 and Mobile to Mobile	A1 and IPsec for HoTI/HoT		A1 and Mobile to Mobile	A1 and IPsec for HoTI/HoT	
	49	RR and BU/BA (Co-Reg, MN1->MN0)	A1 and Mobile to Mobile	A1 and IPsec for HoTI/HoT		A1 and Mobile to Mobile	A1 and IPsec for HoTI/HoT	

	50	ICMP echo request (MN1->MN0) ICMP echo request (MN1->MN0)	A1 and Mobile to Mobile	A1 and IPsec for HoTI/HoT		A1 and Mobile to Mobile	A1 and IPsec for HoTI/HoT	No. 47 and 49

* IKEv1 is out of scope of requirements for "IPv6 Ready Logo Phase2 for MIPv6". However, the IKEv1 specification for MIPv6 is released as an experimental version.

2.4 Examples of “Interoperability test scenario for IPv6 Ready Logo Phase 2 program”

Examples of “Interoperability test scenario for IPv6 Ready Logo Phase 2 program” are shown below.

1) test scenario that includes A1 Architecture of HA/MN (🟦 in Table 2-3)

CN supports IPv6 Function.

HA supports all the Priority A1 in Table 2-1.

MN supports all the Priority A1 in Table 2-1.

-> A operator chooses Functional Units, "A1", in "Required Function" in Table 2-3 (No. 0, 3, 4, 7, 11, 12, 14, 17 and 19).

2) test scenario that includes A1 Architecture of CN (🟦 + 🟩 in Table 2-3)

CN supports all the Priority A1.

HA supports all the Priority A1 and IPsec for HoTI/HoT.

MN supports all the Priority A1 and RR.

-> A operator chooses Functional Unit, "A1", and "A1 and RR (A1 and IPsec for HoTI/HoT)" in "Required Function" in Table 2-3 (No. 0, 3, 4, 6, 7, 8, 11, 12, 13, 14, 15, 17, 18 and 19).

3) test scenario that includes A1 Architecture of CN/HA/MN and Real HL

CN supports all the Priority A1.

HA supports all the Priority A1, Real HL and IPsec for HoTI/HoT.

MN supports all the Priority A1, Real HL and RR.

->A operator chooses Functional Units, "A1", "A1 and Real HL", "A1 and RR (A1 and IPsec for HoTI/HoT)" and "A1, Real HL and RR (A1, Real HL and IPsec for HoTI/HoT)" in "Required Function" in Table 2-3 (No. 0, 3, 4, 6, 7, 8, 11, 12, 13, 14, 15, 17, 18, 19, 26, 27, 28, 29, 30, 31, 32, 35, 36, 38, 39 and 40)

2.5 Test conditions of “Interoperability test scenario for IPv6 Ready Logo Phase 2 program”

The test network topologies and the test procedures of “Interoperability test scenario for IPv6 Ready Logo Phase 2 program” are described in Section 3. The test procedures correspond with Table 2-3. Configuration information, such as IPsec used in “Interoperability test scenario for IPv6 Ready Logo Phase 2 program” is described in Section4. The detailed sequences of “Interoperability test scenario for IPv6 Ready Logo Phase 2 program” are described in Section 3.3. The detailed sequences also correspond with Table 2-3.

For Phase 2 certification, packet logs collected during the test must be submitted, and command logs (e.g. ping) during the test must be submitted in addition to packet logs.

2.6 Compatible conditions for acquisition Phase 2 Logo

Mobile IPv6 equipment (CN, HA, MN (without RR and without Mobile to Mobile)) must execute the “Interoperability test scenario for IPv6 Ready Logo Phase 2 program” with 2 or more different types (different vendors) of equipment to acquire IPv6 Ready Logo Phase 2 program Logo.

MN (with RR and without Mobile to Mobile, with RR and with Mobile to Mobile) must execute the “Interoperability test scenario for IPv6 Ready Logo Phase 2 program” with 4 or more different types (different vendors) of equipment to acquire IPv6 Ready Logo Phase 2 program Logo.

Table 2-4. selection method of a target nodes for “IPv6 Ready Logo Phase 2 program”

candidate node		target nodes		
		CN	HA	MN
CN		-	-	Vendor A,B
HA		-	-	Vendor A,B
MN	w/o RR and w/o Mobile to Mobile	-	Vendor A,B	-
	w/ RR and w/o Mobile to Mobile	Vendor A,B	Vendor C,D	-
	w/ RR and w/ Mobile to Mobile	Vendor A,B	Vendor C,D	*Vendor E,F (Vendor C,D)

* MN of target nodes are selected 2 vendors from Vendor C, D, E, F.

1) In the case where a CN is a candidate for Phase 2 certification

When a CN is a candidate for Phase 2 certification, it must execute the “Interoperability test scenario for IPv6 Ready Logo Phase 2 program” with two or more MNs. The example of the minimum numbers of combinations is shown below.

CN0*---HA0---MN0
CN0*---HA0---MN1
CN0* is a candidate for Phase 2 certification.
HA 0 is a reference for Phase 2 certification.
MN0 and MN1 are target nodes for Phase2 certification. Each target nodes are selected a different vendor.

2) In the case where an HA is a candidate for Phase 2 certification

When an HA is a candidate for Phase 2 certification, it must execute the “Interoperability test scenario for IPv6 Ready Logo Phase 2 program” with two or more MNs. The example of the minimum numbers of combinations is shown below.

CN0---HA0*---MN0
CN0---HA0*---MN1
HA0* is a candidate for Phase 2 certification.
CN0 is a reference for Phase 2 certification.
MN0 and MN1 are target nodes for Phase2 certification. Each target nodes are selected a different vendor.

3) In the case where an MN is a candidate for Phase 2 certification

3-1) Phase 2 certification without RR and without Mobile to Mobile

When an MN is a candidate for Phase 2 certification without RR and without Mobile to Mobile, it must execute “Interoperability test scenario for IPv6 Ready Logo Phase 2 program” with two or more HAs. The example of the minimum number of combinations is shown below.

CN0---HA0---MN0*
CN0---HA1---MN0*
MN0* is a candidate for Phase 2 certification.
CN0 is a reference for Phase 2 certification.
HA0 and HA1 are target nodes for Phase2 certification. Each target nodes are selected a different vendor.

3-2) Phase 2 certification with RR and without Mobile to Mobile

When an MN is a candidate for Phase 2 certification with RR and without Mobile to Mobile, it must execute the “Interoperability test scenario for IPv6 Ready Logo Phase 2 program” with two or more CNs and two or more HAs (total of four or more vendors equipment) . The example of the minimum numbers combinations is shown below.

CN0---HA0---MN0*
CN1---HA1---MN0*
MN0* is a candidate for Phase 2 certification.

CN0, CN1, HA0 and HA1 are target nodes for Phase2 certification. Each target nodes are selected a different vendor.

3-3) Phase 2 certification with RR and with Mobile to Mobile

When an MN is a candidate for Phase 2 certification with RR and with Mobile to Mobile, it must execute the “Interoperability test scenario for IPv6 Ready Logo Phase 2 program” with two or more CNs, two or more HAs, and two or more other MNs (total of four or more vendors equipment). The example of the minimum number combinations is shown below.

```
CN0---HA0---MN0*                  CN0---HA 0 ---MN0*
         |                                  |
                          or
      HA2---MN1                          MN1


CN1---HA1---MN0*                  CN1---HA1---MN0*
         |                                  |
                           or
      HA2---MN2                          MN2
```

MN0* is a candidate for Phase 2 certification.

HA2 is a reference for Phase 2 certification.

CN0, CN1, HA0, HA1, MN1 and MN2 are target nodes for Phase2 certification. Each target nodes are selected according to Table2-4.

2.7 Submission for acquisition of Phase 2 Logo

Submissions for acquisition of Phase 2 Logo are listed

2.7.1 Required data

- **Configuration and information of each node**

(e.g. : the information of node address, link, IPsec and algorithm etc.)

Link

Link[No.]	Link0	Link1	Link2	Link3
Network Address / Prefix				

Example

Link0	Link1
3ffe:0501:ffff:0100::/64	3ffe:0501:ffff:0101::/64

Router

Router[No.]	R0		R1		R2	
Location - Link[No.]	Link0	Link1	Link1	Link2	Link2	Link3
Global Address (IPv6 Address)						
Link Local Address (IPv6 Address)						
MAC address (Ether address)						

R0	
Home-Link0	Foreign-Link1
3ffe:0501:ffff: 0100::1	3ffe:0501:ffff: 0100::2
fe80::1	fe80::2
00:11:11: 11:cn:01	00:11:11: 11:cn:02

Correspondent Node

Node[No.]	CN0
Vender name	
Global Address (IPv6 Address)	
Link Local Address (IPv6 Address)	
MAC address (Ether address)	

CN0
AAA
3ffe:0501:ffff: 0100::1
fe80::0211:11ff: fe11:c101
00:11:11: 11:c1:01

Home Agent

Node[No.]		HA0	HA2
Vender name			
Global Address (IPv6 Address)			
Link Local Address (IPv6 Address)			
MAC address (Ether address)			
Advance functions	RR		
	DHAAD		
	MPD		
	RHL		
IPsec SA	BU/BA	(SPI: /)	(SPI: /)
	RR	(SPI: /)	(SPI: /)
	MPD	(SPI: /)	(SPI: /)
	Payload	Don't use	Don't use
Encryption algorithms		3DES-CBC	3DES-CBC
Authentication algorithms		HMAC-SHA1	HMAC-SHA1

*IPsec SA:the case where IPsec SA of transport mode is divided by BU/BA and MPD, and the case where it is made one are permitted.

HA0	HA2
CCC	DDD
3ffe:0501:ffff: 0100::1	3ffe:0501:ffff: 0100::2
fe80::0211:11ff: fe11:1a01	fe80::0211:11ff: fe11:1a02
00:11:11: 11:1a:01	00:11:11: 11:1a:02
X	X
X	-
X	-
X	X
X (SPI: 273/274)	X (SPI: 529/530)
X (SPI: 275/276)	X (SPI: 531/532)
X (SPI: 277/278)	X (SPI: 533/534)
-	-
3DES-CBC	3DES-CBC, DES-CBC, AES, NULL
HMAC-SHA1	HMAC-SHA1, HMAC-MD5

Mobile Node

Node[No.]		MN0	MN1
Vender name			
Home Address (IPv6 Address)			
Link Local Address (IPv6 Address)			
MAC address (Ether address)			
Care-of Address (FL1)			
Care-of Address (FL2)			
Care-of Address (FL3)			
Advance functions	RR		
	DHAAD		
	MPD		
	RHL		
	Mobile to Mobile		
IPsecSA	BU/BA	(SPI: /)	(SPI: /)
	RR	(SPI: /)	(SPI: /)
	MPD	(SPI: /)	(SPI: /)
	Payload	Don't use	Don't use
Encryption algorithm		3DES-CBC	3DES-CBC
Authentication algorithm		HMAC-SHA1	HMAC-SHA1

MN1	MN2
EEE	FFF
3ffe:0501:ffff: 0100::100	3ffe:0501:ffff: 0100::200
fe80::0211:1111: 1111:2201	fe80::0211:1111: 1111:2202
00:11:11: 11:22:01	00:11:11: 11:22:02
3ffe:0501:ffff: 0101::(Interface id)	3ffe:0501:ffff: 0101::(Interface id)
3ffe:0501:ffff: 0102::(Interface id)	3ffe:0501:ffff: 0102::(Interface id)
3ffe:0501:ffff: 0103::(Interface id)	3ffe:0501:ffff: 0103::(Interface id)
X	X
X	-
X	-
X	X
X	X
X (SPI: 273/274)	X (SPI: 529/530)
X (SPI: 275/276)	X (SPI: 531/532)
X (SPI: 277/278)	X (SPI: 533/534)
-	-
3DES-CBC, NULL	3DES-CBC, DES-CBC, AES, NULL
HAMC-SHA1	HAMC-SHA1, HMAC-MD5

- **Packet Capture File** (e.g. : tcpdump(pcap))

  Save the packet logs on each link.

- **Command Log**

  Save the command logs on each node (e.g. : ping6, ifconfig, ipconfig /all)

- **Topology Map** (see Section 3.1.1)

2.7.2 Test Result Table

Select a candidate node from following parts, and complete each table.

1) In the case where a **CN** is a candidate for Phase 2 certification,

Reference	HA0	
Target	MN0	MN1
CN0		

2) In the case where an **HA** is a candidate for Phase 2 certification,

Reference	CN0	
Target	MN0	MN1
HA0		

3) In the case where an **MN** is a candidate for Phase 2 certification,

3-1) Phase 2 certification without RR and without Mobile to Mobile

Reference	CN0	
Target	HA0	HA1
MN0		

3-2) Phase 2 certification with RR and without Mobile to Mobile

Target	CN0	CN1
Target	HA0	HA1
MN0		

3-3) Phase 2 certification with RR and with Mobile to Mobile

Target	CN0	CN1
Target	HA0 (and HA2)	HA1 (and HA2)
Target	MN1	MN2
MN0		

2.7.3 Data file name syntax

Use following syntax, and name submitted files.

A) Required data (in Section 2.7.1)

Syntax: <Vender-Node>.info

(e.g.: vender1-mn.info)

Syntax: packet_<link No>.dump

(e.g.: packet_link1.dump)

Syntax: command.log

<procedure No.>-<Vender-Node (| _<Vendor-Node>) >-<command>.result

(e.g.: 4_vendor2-MN_address.result
4_vendor3-CN_vendor4-MN_echo.result)

Syntax: topology.map (Option)

B) Test Result Table (in Section 2.7.2)

Syntax: result.tbl

2.7.4 Data Archive

Organize your data as following directory structure.

$Your_Device_ver/Interoperability/result.tbl

$Your_Device_ver/Interoperability/test1/<Vender-Node>.info
$Your_Device_ver/Interoperability/test1/packet_<link No>.dump
$Your_Device_ver/Interoperability/test1/<procedure No.>-<Vender-Node> (| -<Vendor-Node>) -<command>.result
$Your_Device_ver/Interoperability/test1/topology.map

$Your_Device_ver/Interoperability/test2/<Vender-Node>.info
$Your_Device_ver/Interoperability/test2/packet_<link No>.dump
$Your_Device_ver/Interoperability/test2/<procedure No.>-<Vender-Node> (| -<Vendor-Node>) -<command>.result
$Your_Device_ver/Interoperability/test2/topology.map

Put first interoperability data file in "Interoperability/test1/" directry.

Put second interoperability data file in "Interoperability/test2/" directry.

Make a tar.gz archive file, and put files under "$Your_Device_ver" in it.

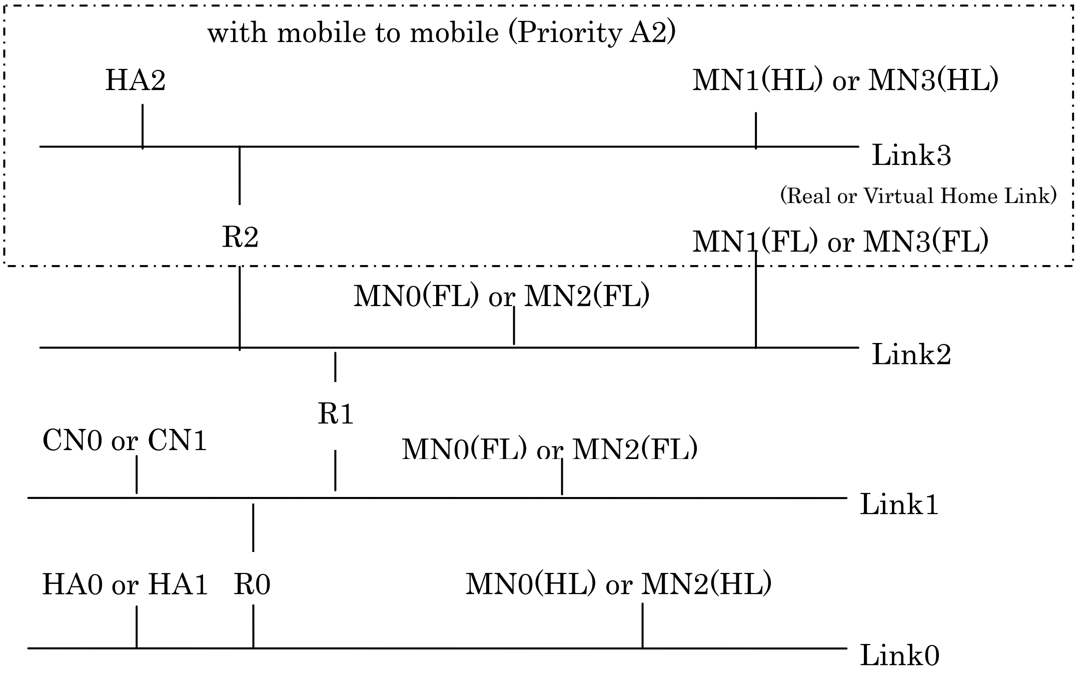
3. Test Procedure for Interoperability test scenario for IPv6 Ready Logo Phase 2

3.1. Test Settings

3.1.1 Topology

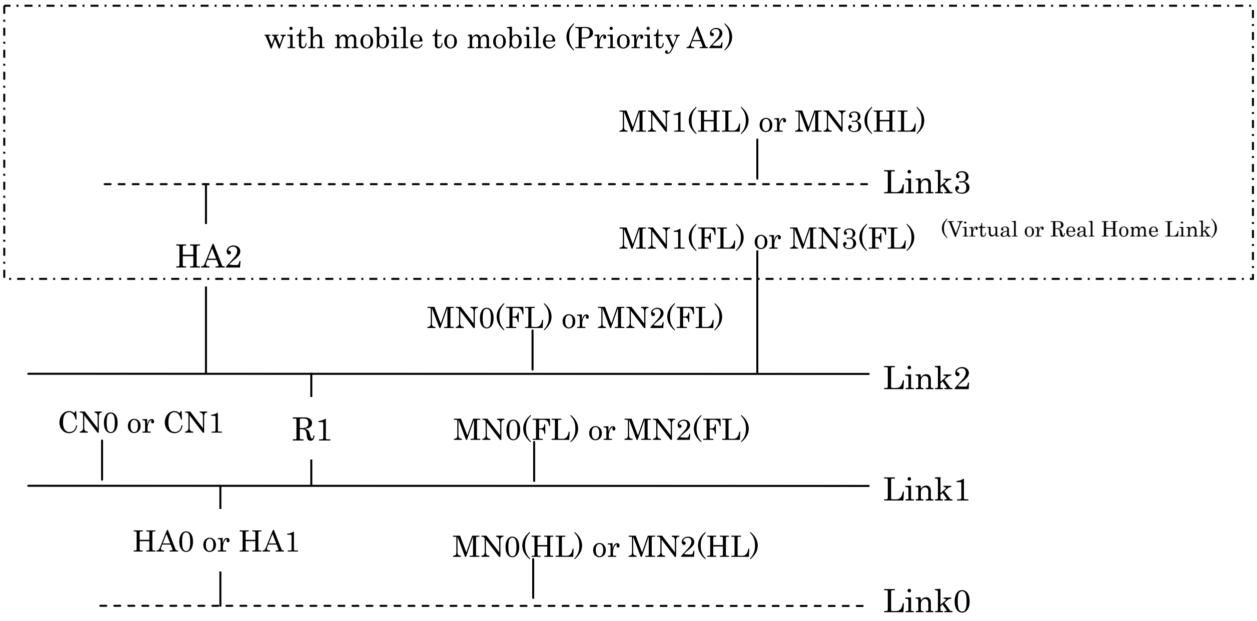
The topologies used in this scenario are shown below. CN, HA and MN are connected as follows. There are two cases of Real Home Link, the setting which HAs have physical home link, and of Virtual Home Link, the setting which HAs do not have physical home link. The example topology of Real Home Link is shown in Section 3.1.1.1, and the example topology of Virtual Home Link is shown in Section 3.1.1.2.

3.1.1.1 Real Home Link



* The number of routers don't be limit. The number of routers can be changed according to the number of interfaces of routers.

3.1.1.2 Virtual Home Link



* The number of routers don't be limit. The number of routers can be changed according to the number of interfaces of routers.

<<Link Information>>

-Link0

3ffe:501:ffff:100::/64

home link for MN0

-Link1

3ffe:501:ffff:101::/64

foreign link for MN0

-Link2

3ffe:501:ffff:102::/64

foreign link for MN0

foreign link for MN1

-Link3

3ffe:501:ffff:103::/64

home link for MN1

<<Node Information>>

-HA0

3ffe:501:ffff:100::200 (Real Home Link)

3ffe:501:ffff:101::1 (Virtual Home Link)

-HA2

3ffe:501:ffff:103::200 (Real Home Link)

3ffe:501:ffff:102::3 (Virtual Home Link)

-MN0(Link0, HL)

3ffe:501:ffff:100::(Interface id) or 3ffe:501:ffff:100::300

Home address

-MN0(Link1, FL)

3ffe:501:ffff:101::(Interface id)

Care-of address

-MN0(Link2, FL)

3ffe:501:ffff:102::(Interface id)

Care-of address

-MN1(Link3,HL)

3ffe:501:ffff:103::(Interface id) or 3ffe:501:ffff:103::301

Home address

-MN1(Link2, FL)

3ffe:501:ffff:102::(Interface id)

Care-of address

-R0(Link0)

3ffe:501:ffff:100::1

-R0(Link1)

3ffe:501:ffff:101::1

-R1(Link1)

3ffe:501:ffff:101::2

-R1(Link2)

3ffe:501:ffff:102::2

-R2(Link2)

3ffe:501:ffff:102::3

-R2(Link3)

3ffe:501:ffff:103::3

-CN0(Link1)

3ffe:501:ffff:101::100

3.1.2 Test Initial conditions

In order to execute this scenario, the following Initial conditions should be satisfied.

* IKEv1 is out of scope of requirements for "IPv6 Ready Logo Phase2 for MIPv6". However, the IKEv1 specification for MIPv6 is released as an experimental version.

(a) CN0

- Does not have BCE for MN0.
- Does not have BCE for MN1.

(b) HA0

- Does not have BCE for MN0.
- The following setting should be configured.

o IPsec : Refer to Section 4(manual configuration or IKE)

(c) HA2

- Does not have BCE for MN1.
- The following setting should be configured.

o IPsec : Refer to Section 4(manual configuration or IKE)

(d) MN0

- Does not have BLE for HA0.
- Does not have BLE for CN0.
- Does not have BLE for MN1.
- Does not have BCE for MN1.
- The following settings should be configured.
  - o HoA : (manual configuration or stateless address autoconfiguration)
  - o HA Address : (manual configuration or DHAAD)
  - o CoA : (stateless address autoconfiguration)
  - o IPsec : Refer to Section 4(manual configuration or IKE)

(e) MN1

- Does not have BLE for HA2.
- Does not have BLE for MN0.
- Does not have BCE for MN0.
- The following settings should be configured.
  - o HoA : (manual configuration or stateless address autoconfiguration)
  - o HA Address : (manual configuration or DHAAD)
  - o CoA : (stateless address autoconfiguration)
  - o IPsec : Refer to Section 4(manual configuration or IKE)

3.2. Test Procedure

3.2.1 Procedure

The procedure executed in this scenario is stated as follows. The procedure can be used in both cases of Real Home Link and Virtual Home Link.

When a Phase 2 Logo applicant is HA, the procedure about HA0 or HA2 is performed.

When a Phase 2 Logo applicant is MN, the procedure about MN0 or MN1 is performed.

When a Phase 2 Logo applicant is CN, the procedure about CN0 is performed.

If you fail the following procedure, you MUST retry the procedure from the first (No.0).

* IKEv1 is out of scope of requirements for “IPv6 Ready Logo Phase2 for MIPv6”. However, the IKEv1 specification for MIPv6 is released as an experimental version.

<<Procedure>>

No.0 Boot up MN under Foreign Link

1 Connect CN0 to Link1.

2 Boot up CN0 under Link1.

=> Save the address information on CN0. (For example, 'ifconfig' Command.)

This file is named '0_ <Vender>-CN _address.result'.

3 Connect HA0 to Link0.

4 Boot up HA0 under Link0.

=> Save the address information on HA0. (For example, 'ifconfig' Command.)

This file is named '0_<Vender>-HA_address.result'.

5 Connect MN0 to Link1 (FL).

6 Boot up MN0 under Link1 (FL).

No.1 DHAAD

1 Transmit an HAAD request from MN0 (Link1, FL) to HA0.

2 Observe an HAAD reply from HA0 to MN0 (Link1, FL).

No.2 IKE phase1 + phase2 (BU/BA)

1 Transmit an IKE phase1 1st message from MN0 (Link1, FL) to HA0.

2 Observe an IKE phase1 2nd message from HA0 to MN0 (Link1, FL).

3 Observe an IKE phase1 3rd message from MN0 (Link1, FL) to HA0.

4 Transmit an IKE phase2 (BU/BA) 1st message from MN0 (Link1, FL) to HA0.

5 Observe an IKE phase2 (BU/BA) 2nd message from HA0 to MN0 (Link1, FL).

6 Observe an IKE phase2 (BU/BA) 3rd message from MN0 (Link1, FL) to HA0.

**If the state of equipment can be displayed, the generated ISAKMP SA and IPsec SA may be verified. (For example, use a command of status display.)

NO.3 BU/BA (Initial Registration)

1 Transmit a BU from MN0 (Link1, FL) to HA0.

2 Observe a BA from HA0 to MN0 (Link1, FL).

=> Save the address information on MN0 for checking HoA and CoA of MN0.

(For example, 'ifconfig' Command.)

This file is named '3_<Vender>-MN_address.result'.

*Verify the other functional unit as follows.

a. If the DHAAD function is selected, verify that destination address of BU is the HA address acquired with DHAAD executed in procedure No.1.

b. If the IKE function is selected, verify that IPsec SA for BU/BA generated with IKE in procedure No.2 are used.

** If the state of equipment can be displayed, the generated BCE and BLE may be verified. (For example, use a command of status display.)

No.4 ICMP echo request (CN->MN)

1 Transmit an ICMPv6 echo request from VENDER-CN to MN0 (Link1, FL).

=> Save the command log on CN0 for ICMPv6 echo. (For example, 'ping6' Command.) This file is named '4_<Vender>-CN _<Vender>-MN_echo.result'.

No.5 IKE phase2 (HoTI/HoT)

1 Transmit an IKE phase2 (HoTI/HoT) 1st message from MN0 (Link1, FL) to HA0.

2 Observe an IKE phase2 (HoTI/HoT) 2nd message from HA0 to MN0 (Link1, FL).

3 Observe an IKE phase2 (HoTI/HoT) 3rd message from MN0 (Link1, FL) to HA0.

** If the state of equipment can be displayed, the generated IPsec SA may be verified. (For example, use a command of status display.)

*** Some implementations will negotiate IKE soon after No.2 procedure. In this case, IKE procedure is not done by this timing

No.6 RR + BU/BA (Co-Reg)

1 Transmit a HoTI from MN0 (Link1, FL) to CN0.

2 Transmit a CoTI from MN0 (Link1, FL) to CN0.

3 Observe a HoT from CN0 to MN0 (Link1, FL).

4 Observe a CoT from CN0 to MN0 (Link1, FL).

5 Transmit a BU (Co-Reg) from MN0 (Link1, FL) to CN0.

(6 Observe a BA from CN0 to MN0 (Link1, FL).)

(If the Acknowledge (A) bit is set in the BU, a BA MUST be sent.)

*Verify the other functional unit as follows.

a. If the RR and IKE function is selected, verify that IPsec SAs for HoTI/HoT generated with IKE in procedure No.5 are used.

** If the state of equipment can be displayed, the generated BCE and BLE may be verified. (For example, use a command of status display.)

No.7 ICMP echo reply (MN->CN)

1 Observe an ICMPv6 echo reply from MN0 (Link1, FL) to CN0.

(Without RR, MN0 sends ICMPv6 echo reply to CN0 via the HA.)

(With RR, MN0 sends ICMPv6 echo reply to CN0 directly, not via the HA.)

*Verify the other functional unit as follows.

a. If the RR function is not selected, verify that CN and MN communicate by BCE created in procedure No.3, via the HA.

b. If the RR function is selected, verify that CN and MN communicate directly by BLE created in procedure No.6, not via the HA.

***Some implementations will communicate via the HA until RR succeeds.

No.8 With RR, ICMP echo request (CN->MN) + ICMP echo reply (MN->CN)

1 Transmit an ICMPv6 echo request from CN0 to MN0 (Link1, FL).

=> Save the command log on CN0 for ICMPv6 echo. (For example, 'ping6' command.)

This file is named '8_<Vender>-CN_<Vender>-MN_echo.result'.

2 Observe an ICMPv6 echo reply from MN0 (Link1, FL) to CN0.

(With RR, CN0 sends ICMPv6 echo request to MN0 directly, not via the HA.)

*Verify the other functional unit as follows.

a. Verify that CN and MN communicate directly by BCE of CN or BLE of MN created in procedure No.6.

No.9 IKE phase2 (MPS/MPA)

1 Transmit an IKE phase2 (MPS/MPA) 1st message from MN0 (Link1, FL) to HA0.

2 Observe an IKE phase2 (MPS/MPA) 2nd message from HA0 to MN0 (Link1, FL).

3 Observe an IKE phase2 (MPS/MPA) 3rd message from MN0 (Link1, FL) to HA0.

** If the state of equipment can be displayed, the generated IPsec SA may be verified.

(For example, use a command of status display.)

*** Some implementations will negotiate IKE soon after No.2 procedure. In this case, IKE procedure is not done by this timing

No.10 MPS/MPA

1 Transmit an MPS from MN0 (Link1, FL) to HA0.

2 Observe an MPA from HA0 to MN0 (Link1, FL).

*Verify the other functional unit as follows.

a. If the MPS/MPA and IKE function is selected, verify that IPsec SA for MPS/MPA generated with IKE in procedure No.9 are used.

***The timing transmitting MPS/MPA is any time after No.3 procedure.

No.11 BU/BA (Re-Reg)

1 MN0 (Link1, FL) stays on the same link and wait.

2 Observe a BU (Re-Reg) to refresh the lifetime from MN0 (Link1, FL) to HA0 before the lifetime of the binding generated in procedure No.3 expires.

3 Observe a BA from HA0 to MN0 (Link1, FL).

** If the state of equipment can be displayed, the updated BCE and BLE may be verified. (For example, use a command of status display.)

No.12 ICMP echo request (CN->MN)

0 If update the BCE of CN and BLE of MN before expire, wait until the RR procedure is done. If don't update the BCE of CN and BLE of MN before expire, wait until the BCE of CN and BLE of MN is deleted.

1 Transmit an ICMPv6 echo request from CN0 to MN0 (Link1, FL).

=> Save the command log on CN0 for ICMPv6 echo. (For example, 'ping6' Command.) This file is named '12_<Vender>-CN_<Vender>-MN_echo.result'.

No.13 RR + BU/BA (Co-Reg)

1 Transmit a HoTI from MN0 (Link1, FL) to CN0.

2 Transmit a CoTI from MN0 (Link1, FL) to CN0.

3 Observe a HoT from CN0 to MN0 (Link1, FL).

4 Observe a CoT from CN0 to MN0 (Link1, FL).

5 Transmit a BU (Co-Reg) from MN0 (Link1, FL) to CN0.

(6 Observe a BA from CN0 to MN0 (Link1, FL).)

(If the Acknowledge (A) bit is set in the BU, a BA MUST be sent.)

** If the state of equipment can be displayed, the generated BCE and BLE may be verified. (For example, use a command of status display.)

***Some implementations update the BCE and BLE before expire. In this case, RR procedure is not done by this timing.

No.14 ICMP echo reply (MN->CN)

1 Observe an ICMPv6 echo reply from MN0 (Link1, FL) to CN0.

(Without RR, MN0 sends ICMPv6 echo reply to CN0 via the HA.)

(With RR, MN0 sends ICMPv6 echo reply to CN0 directly, not via the HA.)

*Verify the other functional unit as follows.

a. If the RR function is not selected, verify that CN and MN communicate by BCE updated in procedure No.11, via the HA.

(A ping6 command log may be used to verify above.)

b. If the RR function is selected, verify that CN and MN communicate directly by BLE updated in procedure No.13, not via the HA.

***Some implementations will communicate via the HA until RR succeeds.

No.15 With RR, ICMP echo request (CN->MN) + ICMP echo reply (MN->CN)

1 Transmit an ICMPv6 echo request from CN0 to MN0 (Link1, FL).

=> Save the command log on CN0 for ICMPv6 echo. (For example, 'ping6' Command.)

This file is named '15_<Vender>-CN_<Vender>-MN_echo.result'.

2 Observe an ICMPv6 echo reply from MN0 (Link1, FL) to CN0.

(With RR, CN0 sends ICMPv6 echo request to MN0 directly, not via the HA.)

*Verify the other functional unit as follows.

a. Verify that CN and MN communicate directly by BCE of CN or BLE of MN updated in procedure No.13.

No.16 IKE phase2 (BU/BA) (Re-keying)

1 MN0 (Link1, FL) stays on the same link and wait.

2 Observe an IKE phase2 (BU/BA) 1st message to refresh the lifetime from MN0 (Link1, FL) to HA0 before the lifetime of the IPsec SA (BU/BA) generated in procedure No.2 expires.

3 Observe an IKE phase2 (BU/BA) 2nd message from HA0 to MN0 (Link1, FL).

4 Observe an IKE phase2 (BU/BA) 3rd message from MN0 (Link1, FL) to HA0.

** If the state of equipment can be displayed, the generated new IPsec SA may be verified. (For example, use a command of status display.)

No.17 BU/BA (Moving)

(0 With RR, if BCE of CN0 and BLE of MN0 have expired, create BCE of CN0 and BLE of MN0 with procedure No. 12-14.)

1 Remove MN0 from Link1 (FL).

2 Connect MN0 to Link2 (FL).

3 Observe a BU from MN0 (Link2, FL) to HA0.

4 Observe a BA from HA0 to MN0 (Link2, FL).

=> Save the address information on MN0 for checking new CoA of MN0.

(For example, 'ifconfig' Command.)

This file is named '17_<Vender>-MN_address.result'.

*Verify the other functional unit as follows.

a. If the IKE function is selected, verify that IPsec SA for BU/BA generated with IKE in procedure No.16 are used.

** If the state of equipment can be displayed, the updated BCE and BLE may be verified.
(For example, use a command of status display.)

No.18 RR + BU/BA (Co-Reg)

(1 Transmit a HoTI from MN0 (Link2, FL) to CN0.)

2 Transmit a CoTI from MN0 (Link2, FL) to CN0.

(3 Observe a HoT from CN0 to MN0 (Link2, FL).)

4 Observe a CoT from CN0 to MN0 (Link2, FL).

5 Transmit a BU (Co-Reg) from MN0 (Link2, FL) to CN0.

(6 Observe a BA from CN0 to MN0 (Link2, FL).)

(If the Acknowledge (A) bit is set in the BU, a BA MUST be sent.)

** If the state of equipment can be displayed, the generated BCE and BLE may be verified.
(For example, use a command of status display.)

No.19 ICMP echo request (CN->MN)

1 Transmit an ICMPv6 echo request from CN0 to MN0 (Link2, FL).

(Without RR, CN0 sends ICMPv6 echo request to MN0 via the HA.)

(With RR, CN0 sends ICMPv6 echo request to MN0 directly, not via the HA.)

=> Save the command log on CN0 for ICMPv6 echo. (For example, 'ping6' Command.)
This file is named '19_<Vender>-CN_<Vender>-MN_echo.result'.

2 Observe an ICMPv6 echo reply from MN0 (Link2, FL) to CN0.

(Without RR, MN0 sends ICMPv6 echo reply to CN0 via the HA.)

(With RR, MN0 sends ICMPv6 echo reply to CN0 directly, not via the HA.)

*Verify the other functional unit as follows.

a. If the RR function is not selected, verify that CN and MN communicate by BCE of HA updated in procedure No.17, via the HA.

b. If the RR function is selected, verify that CN and MN communicate directly by BLE updated in procedure No.18, not via the HA.

No.20 IKE phase2 (BU/BA) or IKE phase1 + phase2 (BU/BA) (Re-keying)

(If the Key Management Mobility Capability (K) bit is supported, skip the following IKE phase1 procedure.)

1 MN0 (Link2, FL) stays on the same link and wait.

(2 Observe an IKE phase1 1st message to refresh the lifetime from MN0 (Link2, FL) to HA0 before the lifetime of the IPsec SA (BU/BA) generated with IKE in procedure No.16 expires.)

(3 Observe an IKE phase1 2nd message from HA0 to MN0 (Link2, FL).)

(4 Observe an IKE phase1 3rd message from MN0 (Link2, FL) to HA0.)

5 Observe an IKE phase2 (BU/BA) 1st message to refresh the lifetime from MN0 (Link2, FL) to HA0 before the lifetime of the IPsec SA (BU/BA) generated with IKE in procedure No.16 expires.

6 Observe an IKE phase2 (BU/BA) 2nd message from HA0 to MN0 (Link2, FL).

7 Observe an IKE phase2 (BU/BA) 3rd message from MN0 (Link2, FL) to HA0.

** If the state of equipment can be displayed, the generated new (ISAKMP SA and) IPsec SA may be verified. (For example, use a command of status display.)

No.21 BU/BA (Moving)

(0 With RR, if BCE of CN0 and BLE of MN0 have expired, create BCE of CN0 and BLE of MN0 with procedure No. 12-14.)

1 Remove MN0 from Link2 (FL).

2 Connect MN0 to Link1 (FL).

3 Observe a BU from MN0 (Link1, FL) to HA0.

4 Observe a BA from HA0 to MN0 (Link1, FL).

=> Save the address information on MN0 for checking new CoA of MN0.

(For example, 'ifconfig' Command.)

This file is named '21_<Vender>-MN_address.result'.

*Verify the other functional unit as follows.

a. If the IKE function is selected, verify that IPsec SA for BU/BA regenerated with IKE in procedure No.20 are used.

** If the state of equipment can be displayed, the updated BCE and BLE may be verified. (For example, use a command of status display.)

No.22 RR + BU/BA (Co-Reg)

1 Transmit a HoTI from MN0 (Link1, FL) to CN0.

2 Transmit a CoTI from MN0 (Link1, FL) to CN0.

3 Observe a HoT from CN0 to MN0 (Link1, FL).

4 Observe a CoT from CN0 to MN0 (Link1, FL).

5 Transmit a BU (Co-Reg) from MN0 (Link1, FL) to CN0.

(6 Observe a BA from CN0 to MN0 (Link1, FL).)

(If the Acknowledge (A) bit is set in the BU, a BA MUST be sent.)

**If the state of equipment can be displayed, the generated BCE and BLE may be verified. (For example, use a command of status display.)

***Some implementations update the BCE and BLE before expire. In this case, RR procedure is not done by this timing.

No.23 ICMP echo request (CN->MN)

1 Transmit an ICMPv6 echo request from CN0 to MN0 (Link1, FL).

(Without RR, CN0 sends ICMPv6 echo request to MN0 via the HA.)

(With RR, CN0 sends ICMPv6 echo request to MN0 directly, not via the HA.)

=> Save the command log on CN0 for ICMPv6 echo. (For example, 'ping6' Command.)

This file is named '23_<Vender>-CN_<Vender>-MN_echo.result'.

No.24 ICMP echo reply (MN->CN)

1 Observe an ICMPv6 echo reply from MN0 (Link1, FL) to CN0.

(Without RR, MN0 sends ICMPv6 echo reply to CN0 via the HA.)

(With RR, MN0 sends ICMPv6 echo reply to CN0 directly, not via the HA.)

*Verify the other functional unit as follows.

a. If the RR function is not selected, verify that CN and MN communicate by BCE of HA updated in procedure No.21, via the HA .

b. If the RR function is selected, verify that CN and MN communicate directly by BLE updated in procedure No.23, not via the HA.

***Some implementations will communicate via the HA until RR succeeds.

No.25 With RR, ICMP echo request (CN->MN) + ICMP echo reply (MN->CN)

1 Transmit an ICMPv6 echo request from CN0 to MN0 (Link1, FL).

=> Save the command log on CN0 for ICMPv6 echo. (For example, 'ping6' Command.)

This file is named '25_<Vender>-CN_<Vender>-MN_echo.result'.

2 Observe an ICMPv6 echo reply from MN0 (Link1, FL) to CN0.

(With RR, CN0 sends ICMPv6 echo request to MN0 directly, not via the HA.)

*Verify the other functional unit as follows.

a. Verify that CN and MN communicate directly by BLE updated in procedure No.23.

No.26 BU/BA (Moving + De-Reg)

(0 With RR, if BCE of CN0 and BLE of MN0 have expired, create BCE of CN0 and BLE of MN0 with procedure No. 12-14.)

1 Remove MN0 from Link1 (FL) or Link2 (FL).

2 Connect MN0 to Link0 (HL).

3 Observe a BU from MN0 (Link0, HL) to HA0.

4 Observe a BA from HA0 to MN0 (Link0, HL).

=> **Save the address information on MN0 for checking address of MN0.**

(For example, 'ifconfig' Command.)

This file is named '26_<Vender>-MN_address.result'.

**If the state of equipment can be displayed, the deleted BCE and BLE may be verified.

(For example, use a command of status display.)

No.27 RR + BU/BA (De-Reg)

1 Transmit a HoTI from MN0 (Link0, HL) to CN0.

2 Observe a HoT from CN0 to MN0 (Link0, HL).

3 Transmit a BU (De-Reg for CN0) from MN0 (Link0, HL) to CN0.

(4 Observe a BA from CN0 to MN0 (Link0, HL).)

(If the Acknowledge (A) bit is set in the BU, a BA MUST be sent.)

**If the state of equipment can be displayed, the deleted BCE and BLE may be verified.

(For example, use a command of status display.)

No.28 ICMP echo request (CN->MN) + ICMP echo reply (MN->CN)

1 Transmit an ICMPv6 echo request from CN0 to MN0 (Link0, HL).

=> **Save the command log on CN0 for ICMPv6 echo. (For example, 'ping6' Command.)**

This file is named '28_<Vender>-CN_<Vender>-MN_echo.result'.

2 Observe an ICMPv6 echo reply from MN0 (Link0, HL) to CN0.

*Verify the other functional unit as follows.

a. Verify that CN and MN communicate directly by deleted BCE of HA, not via the HA.

b. If the RR function is selected, verify that CN and MN communicate directly by deleted BCE of CN.

No.29 Shutdown MN under Home Link

1 Shutdown MN0 (Link0, HL) in the state while connected to HL.

No.30 Boot up MN under Home Link

1 Boot up MN0 (Link0, HL) in the state while connected to HL.

=> **Save the address information on MN0 for checking address.**

(For example, 'ifconfig' Command.)

This file is named '30_<Vender>-MN_address.result'.

No.31 ICMP echo request (CN->MN) + ICMP echo reply (MN->CN)

1 Transmit an ICMPv6 echo request from CN0 to MN0 (Link0, HL).

=> **Save the command log on CN0 for ICMPv6 echo. (For example, 'ping6' Command.)**

This file is named '31_<Vender>-CN_<Vender>-MN_echo.result'.

2 Observe an ICMPv6 echo reply from MN0 (Link0, HL) to CN0.

*Verify the other functional unit as follows.

a. Verify that CN and MN communicate directly, not via the HA.

No.32 Moving

1 Remove MN0 from Link0 (HL).

2 Connect MN0 to Link1 (FL).

No.33 DHAAD

1 Transmit an HAAD request from MN0 (Link1, FL) to HA0.

2 Observe an HAAD reply from HA0 to MN0 (Link1, FL).

No.34 IKE phase1 + phase2 (BU/BA)

1 Transmit an IKE phase1 1st message from MN0 (Link1, FL) to HA0.

2 Observe an IKE phase1 2nd message from HA0 to MN0 (Link1, FL).

3 Observe an IKE phase1 3rd message from MN0 (Link1, FL) to HA0.

4 Transmit an IKE phase2 (BU/BA) 1st message from MN0 (Link1, FL) to HA0.

5 Observe an IKE phase2 (BU/BA) 2nd message from HA0 to MN0 (Link1, FL).

6 Observe an IKE phase2 (BU/BA) 3rd message from MN0 (Link1, FL) to HA0.

**If the state of equipment can be displayed, the generated ISAKMP SA and IPsec SA may be verified. (For example, use a command of status display.)

No.35 BU/BA (Moving)

1 Observe a BU from MN0 (Link1, FL) to HA0.

2 Observe a BA from HA0 to MN0 (Link1, FL).

=> **Save the address information on MN0 for checking new CoA of MN0.**

(For example, 'ifconfig' Command.)

This file is named '35_<Vender>-MN_address.result'.

*Verify the other functional unit as follows.

a. If the DHAAD function is selected, verify that destination address of BU is the HA address acquired with DHAAD executed in procedure No.33.

b. If the IKE function is selected, verify that IPsec SA for BU/BA generated with IKE in procedure No.34 are used.

**If the state of equipment can be displayed, the generated BCE and BLE may be verified.
(For example, use a command of status display.)

No.36 ICMP echo request (CN->MN)

1 Transmit an ICMPv6 echo request from CN0 to MN0 (Link1, FL).

=> Save the command log on CN0 for ICMPv6 echo. (For example, ‘ping6’ Command.)
This file is named ‘36_<Vender>-CN_<Vender>-MN_echo.result’.

No.37 IKE phase2 (HoTI/HoT)

1 Transmit an IKE phase2 (HoTI/HoT) 1st message from MN0 (Link1, FL) to HA0.

2 Observe an IKE phase2 (HoTI/HoT) 2nd message from HA0 to MN0 (Link1, FL).

3 Observe an IKE phase2 (HoTI/HoT) 3rd message from MN0 (Link1, FL) to HA0.

**If the state of equipment can be displayed, the generated IPsec SA may be verified.
(For example, use a command of status display.)

*** Some implementations will negotiate IKE soon after No.34 procedure. In this case, IKE procedure is not done by this timing

No.38 RR + BU/BA (Co-Reg)

1 Transmit a HoTI from MN0 (Link1, FL) to CN0.

2 Transmit a CoTI from MN0 (Link1, FL) to CN0.

3 Observe a HoT from CN0 to MN0 (Link1, FL).

4 Observe a CoT from CN0 to MN0 (Link1, FL).

5 Transmit a BU (Co-Reg) from MN0 (Link1, FL) to CN0.

(6 Observe a BA from CN0 to MN0 (Link1, FL).)
(If the Acknowledge (A) bit is set in the BU, a BA MUST be sent.)

*Verify the other functional unit as follows.

a. If the RR and IKE function is selected, verify that IPsec SA for HoTI/HoT generated with IKE in procedure No.37 are used.

**If the state of equipment can be displayed, the generated BCE and BLE may be verified.
(For example, use a command of status display.)

No.39 ICMP echo reply (MN->CN)

1 Observe an ICMPv6 echo reply from MN0 (Link1, FL) to CN0.
(Without RR, MN0 sends ICMPv6 echo reply to CN0 via the HA.)
(With RR, MN0 sends ICMPv6 echo reply to CN0 directly, not via the HA.)

*Verify the other functional unit as follows.

a. If the RR function is not selected, verify that CN and MN communicate by BCE created in procedure No.35, via the HA.

b. If the RR function is selected, verify that CN and MN communicate directly by BLE created in procedure No.38, not via the HA.

***Some implementations will communicate via the HA until RR succeeds.

No.40 With RR, ICMP echo request (CN->MN) + ICMP echo reply (MN->CN)

1 Transmit anICMPv6 echo request from CN0 to MN0 (Link1, FL).

=> Save the command log on CN0 for ICMPv6 echo. (For example, 'ping6' Command.)

This file is named '40_<Vender>-CN_<Vender>-MN_echo.result'.

2 Observe an ICMPv6 echo reply from MN0 (Link1, FL) to CN0.

(With RR, CN0 sends ICMPv6 echo request to MN0 directly, not via the HA.)

*Verify the other functional unit as follows.

a. Verify that CN and MN communicate directly by BCE of CN or BLE of MN generated in No.38.

No.41 Boot up another MN under Foreign Link

(0 If MN1 belong to the HA0, skip the following boot up procedure of HA2, and consider HA2 as HA0 in the following procedure from No.42 to No. 50.)

(1 Connect HA2 to Link3.)

(2 Boot up HA2 under Link3.)

(=> Save the address information on HA2. (For example, 'ifconfig' Command.)

This file is named '41_<Vender>-HA_address.result'.)

3 Connect MN1 to Link2 (FL).

4 Boot up MN1 under Link2 (FL).

No.42 DHAAD (MN1<=>HA2)

1 Transmit an HAAD request from MN1 (Link2, FL) to HA2.

2 Observe an HAAD reply from HA2 to MN1 (Link2, FL).

No.43 IKE phase1 + phase2 (BU/BA)

1 Transmit an IKE phase1 1st message from MN1 (Link2, FL) to HA2.

2 Observe an IKE phase1 2nd message from HA2 to MN1 (Link2, FL).

3 Observe an IKE phase1 3rd message from MN1 (Link2, FL) to HA2.

4 Transmit an IKE phase2 (BU/BA) 1st message from MN1 (Link2, FL) to HA2.

5 Observe an IKE phase2 (BU/BA) 2nd message from HA2 to MN1 (Link2, FL).

6 Observe an IKE phase2 (BU/BA) 3rd message from MN1 (Link2, FL) to HA2.

**If the state of equipment can be displayed, the generated ISAKMP SA and IPsec SA may be verified. (For example, use a command of status display.)

*** Some implementations will negotiate IKE soon after No.2 procedure. In this case, IKE procedure is not done by this timing

No.44 BU/BA (Initial Registration, MN1<->HA2)

1 Transmit a BU from MN1 (Link2, FL) to HA2.

2 Observe a BA from HA2 to MN1 (Link2, FL).

=> Save the address information on MN1 for checking CoA and HoA of MN1.

(For example, 'ifconfig' Command.)

This file is named '44_<Vender>-MN_address.result'.

**If the state of equipment can be displayed, the generated BCE and BLE may be verified. (For example, use a command of status display.)

No.45 IKE phase2 (HoTI/HoT, MN1<->HA2)

1 Transmit an IKE phase2 (HoTI/HoT) 1st message from MN1 (Link2, FL) to HA2.

2 Observe an IKE phase2 (HoTI/HoT) 2nd message from HA2 to MN1 (Link2, FL).

3 Observe an IKE phase2 (HoTI/HoT) 3rd message from MN1 (Link2, FL) to HA2.

**If the state of equipment can be displayed, the generated IPsec SA may be verified. (For example, use a command of status display.)

*** Some implementations will negotiate IKE soon after No.43 procedure. In this case, IKE procedure is not done by this timing

No.46 ICMP echo request (MN1->MN0)

1 Transmit an ICMPv6 echo request from MN1 (Link2, FL) to MN0 (Link1, FL).

(MN1 sends ICMPv6 echo request to MN0 via the HA2 and HA0.)

=> Save the command log on MN1 for ICMPv6 echo. (For example, 'ping6' Command.)

This file is named '46_<Vender>-MN_<Vender>-MN_echo.result'.

No.47 RR + BU/BA (Co-Reg MN0->MN1)

1 Transmit a HoTI from MN0 (Link1, FL) to MN1 (Link2, FL).

2 Transmit a CoTI from MN0 (Link1, FL) to MN1 (Link2, FL).

3 Observe a HoT from MN1 (Link2, FL) to MN0 (Link1, FL).

4 Observe a CoT from MN1 (Link2, FL) to MN0 (Link1, FL).

5 Transmit a BU (Co-Reg) from MN0 (Link1, FL) to MN1 (Link2, FL).

(6 Observe a BA from MN1 (Link2,FL) to MN0 (Link1, FL).)

(If the Acknowledge (A) bit is set in the BU, a BA MUST be sent.)

**If the state of equipment can be displayed, the generated BCE of MN1 and BLE of MN0 may be verified. (For example, use a command of status display.)

No.48 ICMP echo reply (MN0->MN1)

1 Observe an ICMPv6 echo reply from MN0 (Link1, FL) to MN1 (Link2, FL).

(MN0 sends ICMPv6 echo reply to MN1 via the HA2, not via the HA0.)

***Some implementations will communicate via the HA until RR succeeds.

No.49 RR + BU/BA (Co-Reg MN1->MN0)

1 Transmit a HoTI from MN1 (Link2, FL) to MN0 (Link1, FL).

2 Transmit a CoTI from MN1 (Link2, FL) to MN0 (Link1, FL).

3 Observe a HoT from MN0 (Link1, FL) to MN1 (Link2, FL).

4 Observe a CoT from MN0 (Link1, FL) to MN1 (Link2, FL).

5 Transmit a BU (Co-Reg) from MN1 (Link2, FL) to MN0 (Link1, FL).

(6 Observe a BA from MN0 (Link1, FL) to MN1 (Link2, FL).)

(If the Acknowledge (A) bit is set in the BU, a BA MUST be sent.)

**If the state of equipment can be displayed, the generated BCE of MN0 and BLE of MN1 may be verified. (For example, use a command of status display.)

No.50 ICMP echo request (MN1->MN0) + ICMP echo reply (MN0->MN1)

1 Transmit an ICMPv6 echo request from MN1 (Link2, FL) to MN0 (Link1, FL).

(MN1 sends ICMPv6 echo request to MN0 directly, not via the HA0 and HA2.)

2 Observe an ICMPv6 echo reply from MN0 (Link1, FL) to MN1 (Link2, FL).

(MN0 sends ICMPv6 echo reply to MN1 directly, not via the HA0 and HA2.)

=> Save the command log on MN1 for ICMPv6 echo. (For example, 'ping6' Command.)

This file is named '50_<Vender>-MN_<Vender>-MN_echo.result'.

*Verify the other functional unit as follows.

a. Verify that MN0 and MN1 communicate directly by BCE or BLE of each MN updated in procedure No.47 and 49.

3.2.2 Procedure of verifying test scenario

Mobile IPv6 sequence under the actual execution of this scenario is described in Section 3.3. Check that sequences in the log are the same as that in Section 3.3.

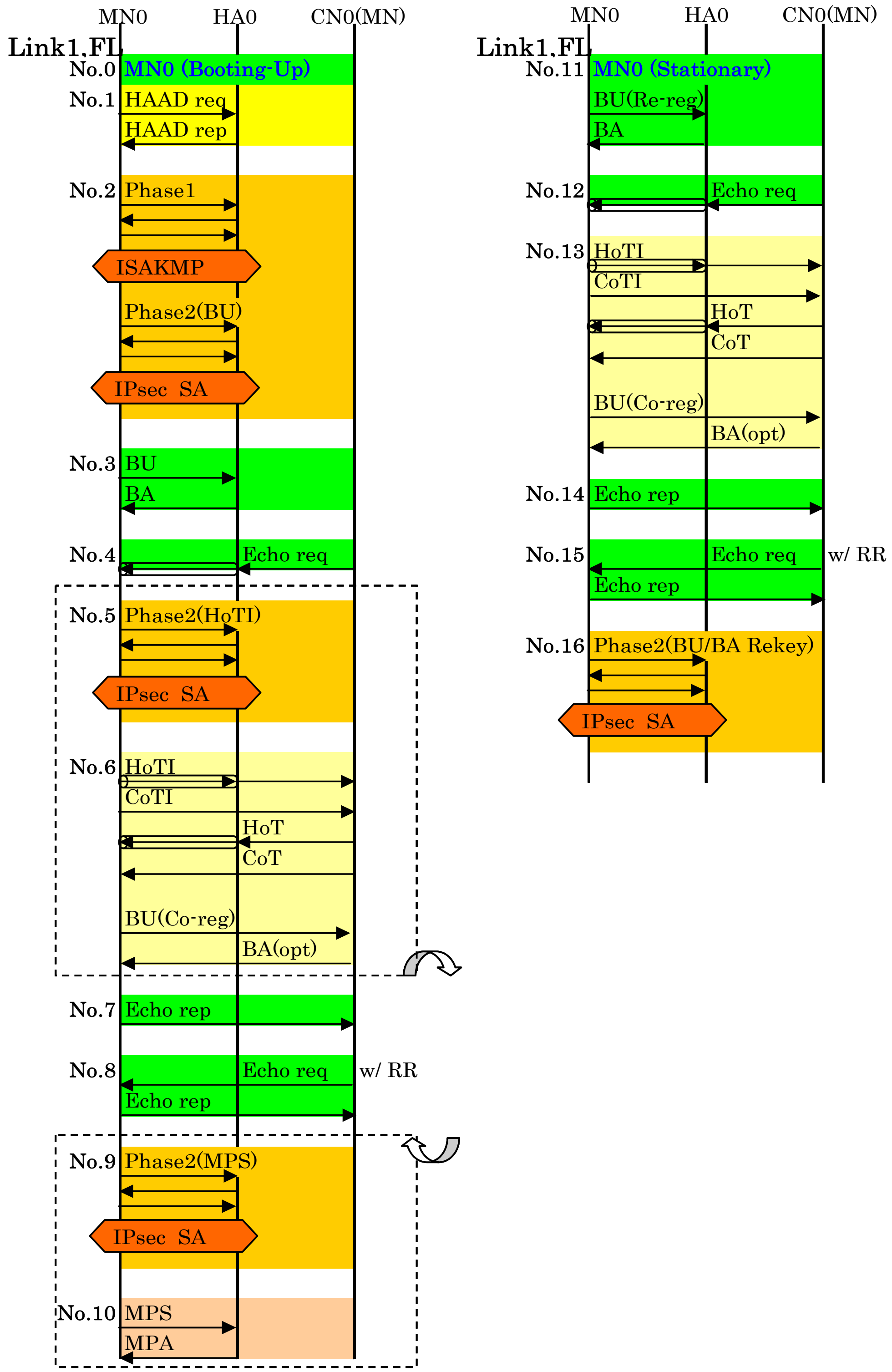
The check should be executed at the stage whichever of the following 'A' or 'B'.

A. Under each procedure of Section 3.2.1

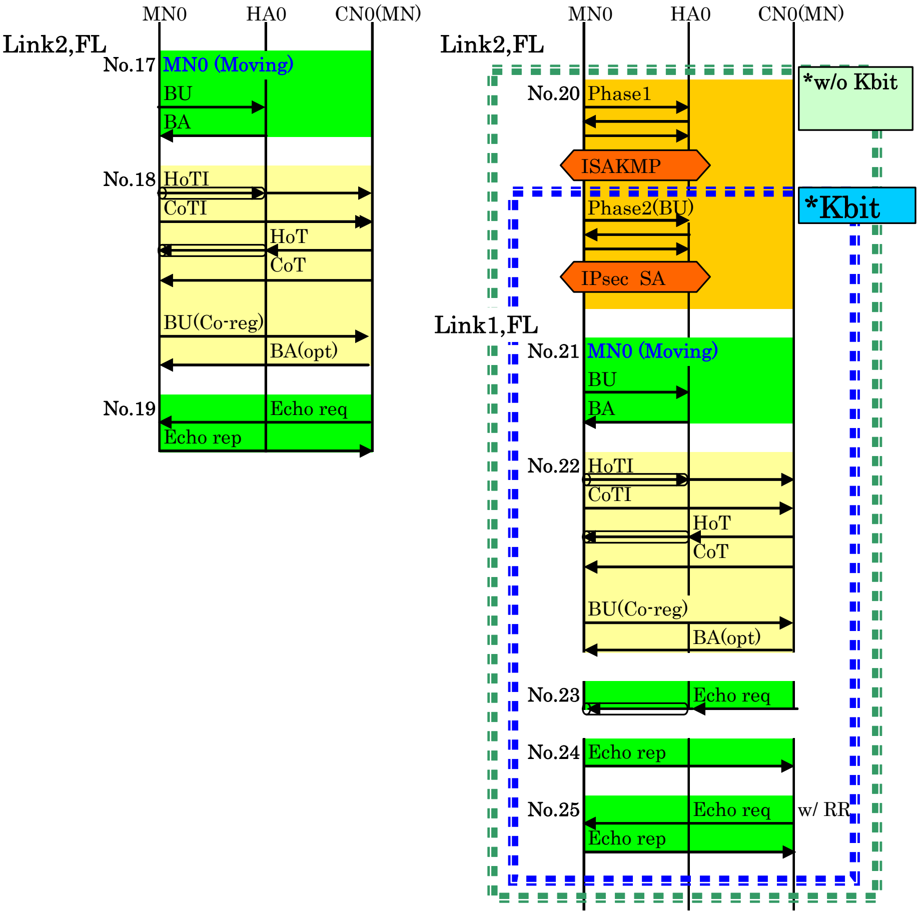
B. After executing test scenario

3.3 Scequence of Interoperability Test Scenario

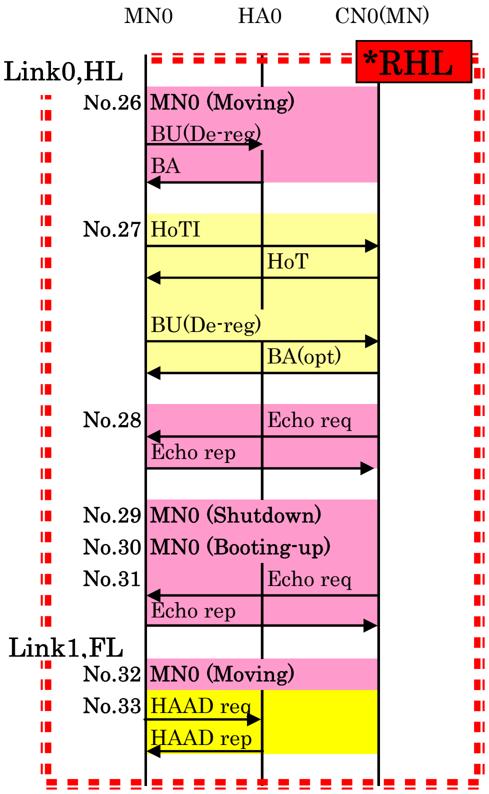
Sequence of Interoperability Test Scenario(1/4)

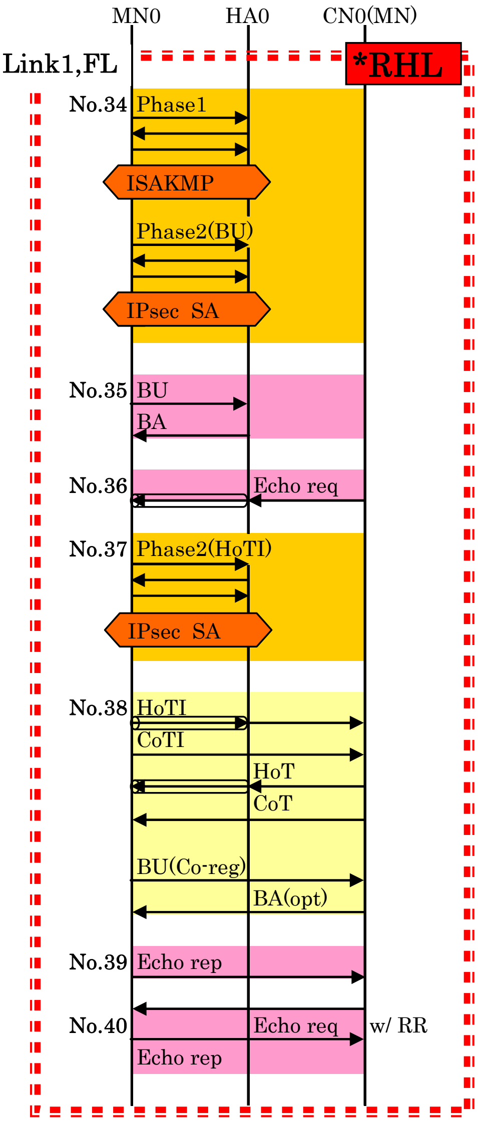


Sequence of Interoperability Test Scenario(2/4)

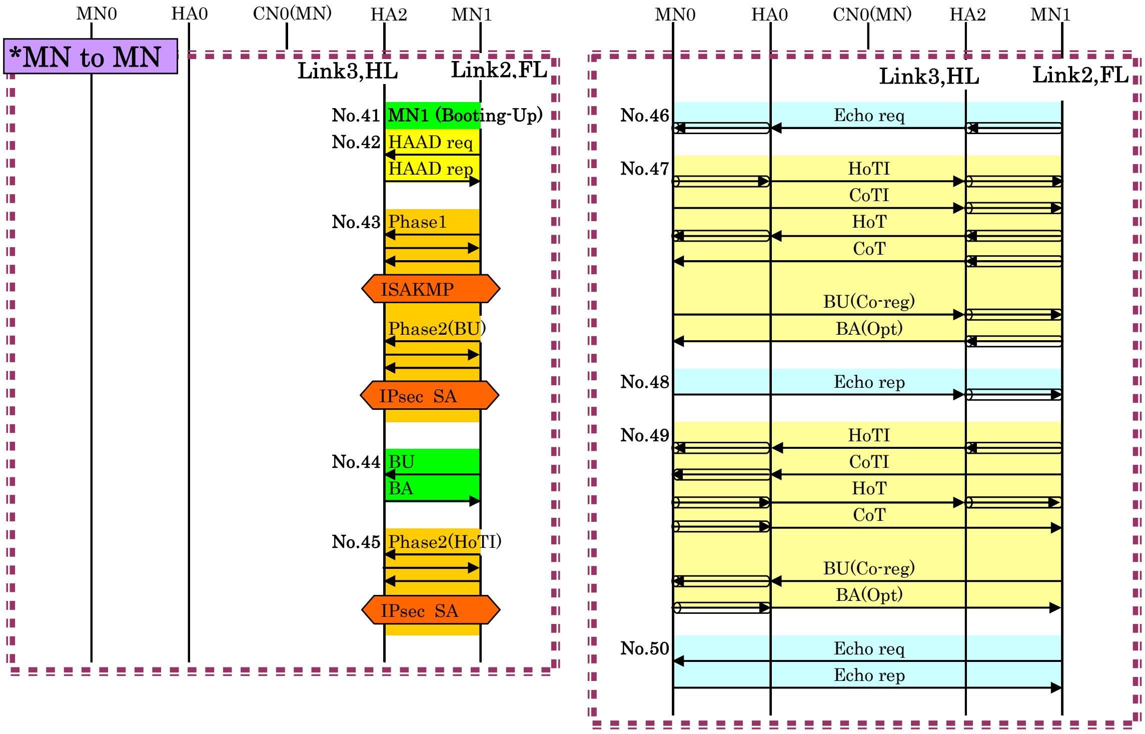


Sequence of Interoperability Test Scenario(3/4)





Sequence of Interoperability Test Scenario(4/4)



* IKEv1 is out of scope of requirements for “IPv6 Ready Logo Phase2 for MIPv6”. However, the IKEv1 specification for MIPv6 is released as an experimental version.

4. Various lifetimes and IPsec/IKE configurations

4.1. Various lifetimes configurations

In order to execute this scenario, various lifetimes are set as follows.

* IKEv1 is out of scope of requirements for "IPv6 Ready Logo Phase2 for MIPv6". However, the IKEv1 specification for MIPv6 is released as an experimental version.

Binding Cache	
-Home Registration	420 seconds
Return Routability	
-nonce	240 seconds
-token	210 seconds
-Correspondent Registration	270 seconds
IKE	
-ISAKMP SA	28800 seconds
-IPsec SA(BU/BA)	840 seconds
-IPsec SA(HoTI/HoT)	840 seconds
-IPsec SA(MPS/MPA)	840 seconds
-IPsec SA(Payload)*	840 seconds

*The IPsec SA(Payload) is for development. It is not used in the interoperability test scenario.

4.2. IPsec/IKE configurations

In order to test with manual configurations of IPsec SA, the IPsec configurations are set as described in Section 4.3. In order to test with IKE, the IKE configurations are set as described in Section 4.4.

4.3. Manual IPsec SA configurations

SPD and SAD entries to protect BU/BA, HoTI/HoT, MPS/MPA and Payload packets between HA and MN is described below.

According to RFC3776, the case where IPsec SAs for transport mode are divided by BU/BA and MPD, and the case where two IPsec SAs are grouped and made one are permitted.

But in case of executing "Interoperability test scenario for IPv6 Ready Logo Phase 2 program", considering the interoperability, IPsec SAs must be divided by BU/BA, MPD and HoTI/HoT. (see Section 2.3.3 in Guidelines for Implementation)

In case of executing "Interoperability test scenarios for implementers", IPsec SAs may be grouped and made one.

Moreover, when IPsec SAs for transport mode are made one, IPsec SA configurations for BU/BA are used (see Section 4.3.1). ("Any" is set as Transport Layer Protocol.) When IPsec SAs for tunnel mode are made one, IPsec SA configurations for Payload are used (see Section 4.3.4). ("Any" is set as Transport Layer Protocol.)

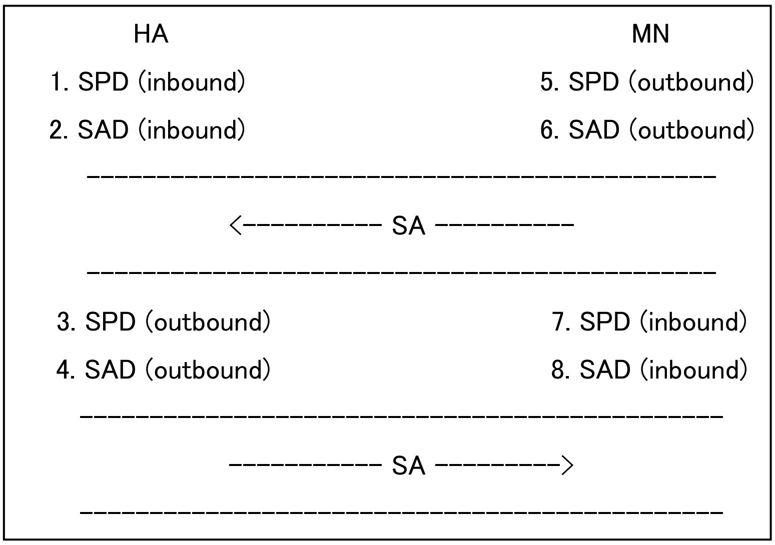


Figure 4.1 Manual IPsec SA configurations between HA and MN

4.3.1. BU/BA [Transport Mode] for manual IPsec SA

<SPD for HA (inbound) and MN (outbound) (refer to 1 and 5 in Figure 4.1)>

Source Address	MN Home Address
Destination Address	HA Address
IPsec Protocol	ESP
Transport Layer Protocol	MH
IPsec protocol mode	transport mode

<SPD for HA (outbound) and MN (inbound) (refer to 3 and 7 in Figure 4.1)>

Source Address	HA Address
Destination Address	MN Home Address
IPsec Protocol	ESP
Transport Layer Protocol	MH
IPsec protocol mode	transport mode

<SA1 for HA (inbound) and MN (outbound) (refer to 2 and 6 in Figure 4.1)>

	MN0	HA0	MN1	HA2
Source Address	MN Home Address	MN Home Address	MN Home Address	MN Home Address
Destination Address	HA Address	HA Address	HA Address	HA Address
IPsec Protocol	ESP	ESP	ESP	ESP
SPI	0x111	0x111	0x221	0x221
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96
Authentication keys	V6LC-111--1234567890	V6LC-111--1234567890	V6LC-221--1234567890	V6LC-221--1234567890
Encryption algorithm	3DES-CBC	3DES-CBC	3DES-CBC	3DES-CBC
Encryption keys	V6LC-111--12345678901234	V6LC-111--12345678901234	V6LC-221--12345678901234	V6LC-221--12345678901234

<SA2 for HA (outbound) and MN (inbound) (refer to 4 and 8 in Figure 4.1)>

	MN0	HA0	MN1	HA2
Source Address	HA Address	HA Address	HA Address	HA Address
Destination Address	MN Home Address	MN Home Address	MN Home Address	MN Home Address
IPsec Protocol	ESP	ESP	ESP	ESP
SPI	0x112	0x112	0x222	0x222
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96
Authentication keys	V6LC-112--1234567890	V6LC-112--1234567890	V6LC-222--1234567890	V6LC-222--1234567890
Encryption algorithm	3DES-CBC	3DES-CBC	3DES-CBC	3DES-CBC
Encryption keys	V6LC-112--12345678901234	V6LC-112--12345678901234	V6LC-222--12345678901234	V6LC-222--12345678901234

** HMAC-SHA1-96 and 3DES-CBC must be selected as Authentication algorithm and Encryption algorithm in “Interoperability test scenario for IPv6 Ready Logo Phase 2 program”

4.3.2. HoTI/HoT[Tunnel Mode] for manual IPsec SA

<SPD for HA (inbound) and MN (outbound) (refer to 1 and 5 in Figure 4.1)>

Source Address	MN Home Address
Destination Address	Any
IPsec Protocol	ESP
Transport Layer Protocol	MH(*)
IPsec protocol mode	tunnel mode

<SPD for HA (outbound) and MN (inbound) (refer to 3 and 7 in Figure 4.1)>

Source Address	Any
Destination Address	MN Home Address
IPsec Protocol	ESP
Transport Layer Protocol	MH(*)
IPsec protocol mode	tunnel mode

(*)In case of executing “Interoperability test scenario for IPv6 Ready Logo Phase 2 program”, “MH” is set as the Transport Layer Protocol of an IPsec selector.

If MH message type is supported, “Any” is set as MH message type.

<SA3 for HA (inbound) and MN (outbound) (refer to 2 and 6 in Figure 4.1)>

	MN0	HA0	MN1	HA2
Outer Source Address	MN Care of Address	MN Care of Address	MN Care of Address	MN Care of Address
Outer Destination Address	HA Address	HA Address	HA Address	HA Address
Inner Source Address	MN Home Address	MN Home Address	MN Home Address	MN Home Address
Inner Destination Address	Any	Any	Any	Any
IPsec	ESP	ESP	ESP	ESP

Protocol				
SPI	0x113	0x113	0x223	0x223
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96
Authentication keys	V6LC-113--1234567890	V6LC-113--1234567890	V6LC-223--1234567890	V6LC-223--1234567890
Encryption algorithm	3DES-CBC	3DES-CBC	3DES-CBC	3DES-CBC
Encryption keys	V6LC-113--12345678901234	V6LC-113--12345678901234	V6LC-223--12345678901234	V6LC-223--12345678901234

<SA4 for HA (outbound) and MN (inbound) (refer to 4 and 8 in Figure 4.1)>

	MN0	HA0	MN1	HA2
Outer Source Address	HA Address	HA Address	HA Address	HA Address
Outer Destination Address	MN Care of Address	MN Care of Address	MN Care of Address	MN Care of Address
Inner Source Address	Any	Any	Any	Any
Ineer Destination Address	MN Home Address	MN Home Address	MN Home Address	MN Home Address
IPsec Protocol	ESP	ESP	ESP	ESP
SPI	0x114	0x114	0x224	0x224
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96
Authentication keys	V6LC-114--1234567890	V6LC-114--1234567890	V6LC-224--1234567890	V6LC-224--1234567890
Encryption	3DES-CBC	3DES-CBC	3DES-CBC	3DES-CBC

algorithm				
Encryption keys	V6LC-114--12345678901234	V6LC-114--12345678901234	V6LC-224--12345678901234	V6LC-224--12345678901234

** HMAC-SHA1-96 and 3DES-CBC must be selected as Authentication algorithm and Encryption algorithm in “Interoperability test scenario for IPv6 Ready Logo Phase 2 program”

4.3.3. MPS/MPA [Transport Mode] for manual IPsec SA

<SPD for HA (inbound) and MN (outbound) (refer to 1 and 5 in Figure 4.1)>

Source Address	MN Home Address
Destination Address	HA Address
IPsec Protocol	ESP
Transport Layer Protocol	ICMPv6 (*)
IPsec protocol mode	transport mode

<SPD for HA (outbound) and MN (inbound) (refer to 3 and 7 in Figure 4.1)>

Source Address	HA Address
Destination Address	MN Home Address
IPsec Protocol	ESP
Transport Layer Protocol	ICMPv6 (*)
IPsec protocol mode	transport mode

(*)In case of executing “Interoperability test scenario for IPv6 Ready Logo Phase 2 program”, “ICMPv6” is set as the Transport Layer Protocol of an IPsec selector. If ICMPv6 message type is supported, “Any” is set as ICMPv6 message type.

<SA5 for HA (inbound) and MN (outbound) (refer to 2 and 6 in Figure 4.1)>

	MN0	HA0	MN1	HA2
Source Address	MN Home Address	MN Home Address	MN Home Address	MN Home Address
Destination Address	HA Address	HA Address	HA Address	HA Address
IPsec Protocol	ESP	ESP	ESP	ESP
SPI	0x115	0x115	0x225	0x225
Authentica	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96

tion algorithm				
Authentication keys	V6LC-115--1234567890	V6LC-115--1234567890	V6LC-225--1234567890	V6LC-225--1234567890
Encryption algorithm	3DES-CBC	3DES-CBC	3DES-CBC	3DES-CBC
Encryption keys	V6LC-115--12345678901234	V6LC-115--12345678901234	V6LC-225--12345678901234	V6LC-225--12345678901234

<SA6 for HA (outbound) and MN (inbound) (refer to 4 and 8 in Figure 4.1)>

	MN0	HA0	MN1	HA2
Source Address	HA Address	HA Address	HA Address	HA Address
Destination Address	MN Home Address	MN Home Address	MN Home Address	MN Home Address
IPsec Protocol	ESP	ESP	ESP	ESP
SPI	0x116	0x116	0x226	0x226
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96
Authentication keys	V6LC-116--1234567890	V6LC-116--1234567890	V6LC-226--1234567890	V6LC-226--1234567890
Encryption algorithm	3DES-CBC	3DES-CBC	3DES-CBC	3DES-CBC
Encryption keys	V6LC-116--12345678901234	V6LC-116--12345678901234	V6LC-226--12345678901234	V6LC-226--12345678901234

** HMAC-SHA1-96 and 3DES-CBC must be selected as Authentication algorithm and Encryption algorithm in "Interoperability test scenario for IPv6 Ready Logo Phase 2 program"

4.3.4. Payload [Tunnel Mode] for manual IPsec SA

This configuration is for development. It is not used in "Interoperability test scenario for IPv6 Ready Logo Phase 2 program"

<SPD for HA (inbound) and MN (outbound) (refer to 1 and 5 in Figure 4.1)>

Source Address	MN Home Address
Destination Address	Any
IPsec Protocol	ESP
Transport Layer Protocol	Any
IPsec protocol mode	Transport mode

<SPD for HA (outbound) and MN (inbound) (refer to 3 and 7 in Figure 4.1)>

Source Address	MN Home Address
Destination Address	Any
IPsec Protocol	ESP
Transport Layer Protocol	Any
IPsec protocol mode	Transport mode

<SA7 for HA (inbound) and MN (outbound) (refer to 2 and 6 in Figure 4.1)>

	MN0	HA0	MN1	HA2
Outer Source Address	MN Care of Address	MN Care of Address	MN Care of Address	MN Care of Address
Outer Destination Address	HA Address	HA Address	HA Address	HA Address
Inner Source Address	MN Home Address	MN Home Address	MN Home Address	MN Home Address
Inner Destination Address	Any	Any	Any	Any
IPsec Protocol	ESP	ESP	ESP	ESP
SPI	0x117	0x117	0x227	0x227
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96
Authentication keys	V6LC-117--1234567890	V6LC-117--1234567890	V6LC-227--1234567890	V6LC-227--1234567890

Encryption algorithm	3DES-CBC	3DES-CBC	3DES-CBC	3DES-CBC
Encryption keys	V6LC-117--12345678901234	V6LC-117--12345678901234	V6LC-227--12345678901234	V6LC-227--12345678901234

<SA8 for HA (outbound) and MN (inbound) (refer to 4 and 8 in Figure 4.1)>

	MN0	HA0	MN1	HA2
Outer Source Address	HA Address	HA Address	HA Address	HA Address
Outer Destination Address	MN Care of Address	MN Care of Address	MN Care of Address	MN Care of Address
Inner Source Address	Any	Any	Any	Any
Inner Destination Address	MN Home Address	MN Home Address	MN Home Address	MN Home Address
IPsec Protocol	ESP	ESP	ESP	ESP
SPI	0x118	0x118	0x228	0x228
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96
Authentication keys	V6LC-118--1234567890	V6LC-118--1234567890	V6LC-228--1234567890	V6LC-228--1234567890
Encryption algorithm	3DES-CBC	3DES-CBC	3DES-CBC	3DES-CBC
Encryption keys	V6LC-118--12345678901234	V6LC-118--12345678901234	V6LC-228--12345678901234	V6LC-228--12345678901234

Reference: Calculation method of SPI, Authentication keys and Encryption keys for Manual IPsec SA between HA and MN

- Calculation method of SPI

SPI = (HA-No+1) * 0x100 + (MN-No+1) * 0x10 + SA-№

Example:

1) [HA-No=0] : [MN-No=0] : [SA-No=1]

0x100 + 0x10 + 0x1 = 0x111

2) [HA-No=1] : [MN-No=1] : [SA-No=4]

0x200 + 0x20 + 0x4 = 0x224

- Selection method of Authentication keys

Relation between Algorithm and Key is shown below.

Algorithm	Key (<SPI> is SPI number(HEX))
HMAC-SHA1	V6LC-<SPI>--1234567890
HMAC-MD5	V6LC-<SPI>--123456
NULL	(none)

Example:

1) [HA-No=0] <- [MN-No=1]: [SA-No=1] (HMAC-SHA1)

0x100 + 0x20 + 0x1 = 0x121

Key = 'V6LC-121--1234567890'

- Selection method of Encryption keys

Relation between Algorithm and Key is shown below.

Algorithm	Key (<SPI> is the base on HEX)
3DES-CBC	V6LC-<SPI>--12345678901234
DES-CBC	V6LC-<SPI>
NULL	(none)

Example:

1) [HA-No=1] <- [MN-No=1]: [SA-No=1] (3DES-CBC)

0x200 + 0x20 + 0x1 = 0x221

Key = 'V6LC-221--12345678901234'

4.4. IKE configurations

SPD and IKE phase 1/phase 2 to protect BU/BA, HoTI/HoT, MPS/MPA and Payload packets between HA and MN are described below.

But in case of executing "Interoperability test scenario for IPv6 Ready Logo Phase 2 program", considering the interoperability, IPsec SAs must be divided by BU/BA, MPS/MPA and HoTI/HoT. (see Section 2.3.3 in Guidelines for Implementation)

In case of executing "Interoperability test scenarios for implementers", IPsec SAs may be grouped and made one.

Moreover, when IPsec SAs for transport mode are made one, IKE configurations for BU/BA are used (see Section 4.4.2). ("Any" is set as Transport Layer Protocol.) When IPsec SAs for tunnel mode are made one, IKE configurations for Payload are used (see Section 4.4.5). ("Any" is set as Transport Layer Protocol.)

* IKEv1 is out of scope of requirements for "IPv6 Ready Logo Phase2 for MIPv6". However, the IKEv1 specification for MIPv6 is released as an experimental version.

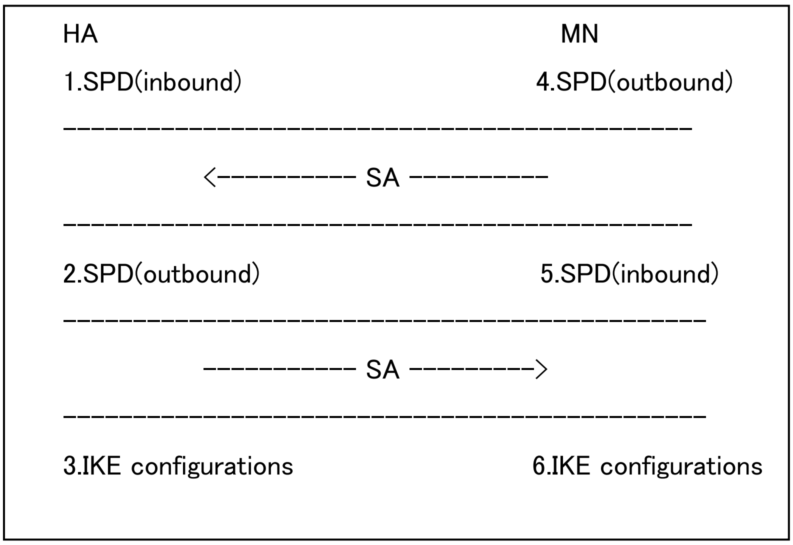


Figure 4.2 IKE configurations between HA and MN

4.4.1. IKE phase1 configurations

<IKE phase1 for MN and HA (refer to 3 and 6 in Figure 4.2)>

	MN0	HA0	MN1	HA2
Hash algorithm	SHA1-96	SHA1-96	SHA1-96	SHA1-96
Encryption algorithm	3DES-CBC	3DES-CBC	3DES-CBC	3DES-CBC
Authentication method	Pre-Shared key	Pre-Shared key	Pre-Shared key	Pre-Shared key
Group Description	MODP Group 2	MODP Group 2	MODP Group 2	MODP Group 2
Life Type	Second	Second	Second	Second
Life Duration	28800	28800	28800	28800
Pre-Shared key	V6LC-11--1234567890	V6LC-11--1234567890	V6LC-11--1234567890	V6LC-11--1234567890
ID Type	FQDN or User FQDN	FQDN or User FQDN	FQDN or User FQDN	FQDN or User FQDN
Identification Data	mn0.ha0.net or mn0@ha0.net	ha0.ha0.net or ha0@ha0.net	mn1.ha2.net or mn1@ha2.net	Ha2.ha2.net or Ha2@ha2.net

** SHA1-96, 3DES-CBC and MODP Group2 must be selected as Hash algorithm, Encryption algorithm and Group Description in the "Interoperability test scenario for IPv6 Ready Logo Phase 2 program".

Reference: Calculation method of Pre-Shared keys and Identification Data for IKE Phase 1 configurations between HA and MN

- Selection method of Pre-Shared key between HA and MN

Pre-shared Key is shown below.
Pre-shared Key V6LC-<[HA-No][MN-No]>--1234567890

Example:
1) [HA-No=1] [MN-No=1]: 0x11
Key = V6LC-11--1234567890

- Selection method of Identification Data between HA and MN

Relation between Identification Data Type and Identification Data is shown below.

MN

FQDN	mn<[MN-No]>.ha<[HA-No]>.net
User FQDN	mn<[MN-No]>@ha<[HA-No]>.net

HA

FQDN	ha<[HA-No]>.ha<[HA-No]>.net
User FQDN	ha<[HA-No]>@ha<[HA-No]>.net

Example:

1) [HA-No=0] [MN-No=0]:

MN's FQDN = mn1.ha2.net
MN's User FQDN = mn1@ha2.net
HA's FQDN = ha2.ha2.net
HA's User FQDN = ha2@ha2.net

4.4.2. BU/BA [Transport Mode]

<SPD for HA (inbound) and MN (outbound) (refer to 1 and 4 in Figure 4.2)>

Source Address	MN Home Address
Destination Address	HA Address
IPsec Protocol	ESP
Transport Layer Protocol	MH
IPsec protocol mode	transport mode

<SPD for HA (outbound) and MN (inbound) (refer to 2 and 5 in Figure 4.2)>

Source Address	HA Address
Destination Address	MN Home Address
IPsec Protocol	ESP
Transport Layer Protocol	MH
IPsec protocol mode	transport mode

<IKE phase2 for MN and HA (refer to 3 and 6 in Figure 4.2)>

	MN0	HA0	MN1	HA2
IPsec Protocol	ESP	ESP	ESP	ESP
Encryption algorithm	3DES-CBC	3DES-CBC	3DES-CBC	3DES-CBC
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96
Life Type	Second	Second	Second	Second
Life Duration	840	840	840	840
Encapsulation Mode	transport mode	transport mode	transport mode	transport mode
Initiator ID Type	ID_IPV6_ADDR	ID_IPV6_ADDR	ID_IPV6_ADDR	ID_IPV6_ADDR
Initiator ID protocol	MH	MH	MH	MH
Initiator Identification Data	MN Home Address	MN Home Address	MN Home Address	MN Home Address
Responder ID Type	ID_IPV6_ADDR	ID_IPV6_ADDR	ID_IPV6_ADDR	ID_IPV6_ADDR
Responder ID protocol	MH	MH	MH	MH
Responder Identification Data	HA Address	HA Address	HA Address	HA Address

* w/o Perfect Forward Secrecy (PFS) in IKE Phase 2

** HMAC-SHA1-96 and 3DES-CBC must be selected as Authentication algorithm and Encryption algorithm in "Interoperability test scenario for IPv6 Ready Logo Phase 2 program"

4.4.3. HoTI/HoT [Tunnel Mode]

<SPD for HA (inbound) and MN (outbound) (refer to 1 and 4 in Figure 4.2)>

Source Address	MN Home Address
Destination Address	Any
IPsec Protocol	ESP

Transport Layer Protocol	MH(*)
IPsec protocol mode	tunnel mode

<SPD for HA (outbound) and MN (inbound) (refer to 2 and 5 in Figure 4.2)>

Source Address	Any
Destination Address	MN Home Address
IPsec Protocol	ESP
Transport Layer Protocol	MH(*)
IPsec protocol mode	tunnel mode

(*)In case of executing “Interoperability test scenario for IPv6 Ready Logo Phase 2 program”, “MH” is set as the Transport Layer Protocol of an IPsec selector.
If MH message type is supported, “Any” is set as MH message type.

<IKE phase2 for MN and HA (refer to 3 and 6 in Figure 4.2)>

	MN0	HA0	MN1	HA2
IPsec Protocol	ESP	ESP	ESP	ESP
Encryption algorithm	3DES-CBC	3DES-CBC	3DES-CBC	3DES-CBC
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96
Life Type	Second	Second	Second	Second
Life Duration	840	840	840	840
Encapsulation Mode	tunnel mode	tunnel mode	tunnel mode	tunnel mode
Initiator ID Type	ID_IPV6_ADDR	ID_IPV6_ADDR	ID_IPV6_ADDR	ID_IPV6_ADDR
Initiator ID protocol	MH	MH	MH	MH
Initiator Identification Data	MN Home Address	MN Home Address	MN Home Address	MN Home Address
Responder ID Type	ID_IPV6_ADDR _SUBNET	ID_IPV6_ADDR _SUBNET	ID_IPV6_ADDR _SUBNET	ID_IPV6_ADDR _SUBNET
Responder ID protocol	MH	MH	MH	MH

Responder Identification Data	0 (Any)	0 (Any)	0 (Any)	0 (Any)

* w/o Perfect Forward Secrecy (PFS) in IKE Phase 2

** HMAC-SHA1-96 and 3DES-CBC must be selected as Authentication algorithm and Encryption algorithm in “Interoperability test scenario for IPv6 Ready Logo Phase 2 program”

4.4.4. MPS/MPA [Transport Mode]

<SPD for HA (inbound) and MN (outbound) (refer to 1 and 4 in Figure 4.2)>

Source Address	MN Home Address
Destination Address	HA Address
IPsec Protocol	ESP
Transport Layer Protocol	ICMPv6 (*)
IPsec protocol mode	transport mode

<SPD for HA (outbound) and MN (inbound) (refer to 2 and 5 in Figure 4.2)>

Source Address	HA Address
Destination Address	MN Home Address
IPsec Protocol	ESP
Transport Layer Protocol	ICMPv6 (*)
IPsec protocol mode	transport mode

(*)In case of executing “Interoperability test scenario for IPv6 Ready Logo Phase 2 program”, “ICMPv6” is set as the Transport Layer Protocol of an IPsec selector.
If ICMPv6 message type is supported, “Any” is set as ICMPv6 message type.

<IKE phase2 for MN and HA (refer to 3 and 6 in Figure 4.2)>

	MN0	HA0	MN1	HA2
IPsec Protocol	ESP	ESP	ESP	ESP
Encryption algorithm	3DES-CBC	3DES-CBC	3DES-CBC	3DES-CBC
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96
Life Type	Second	Second	Second	Second
Life Duration	840	840	840	840

Encapsulation Mode	transport mode	transport mode	transport mode	transport mode
Initiator ID Type	ID_IPV6_ADDR	ID_IPV6_ADDR	ID_IPV6_ADDR	ID_IPV6_ADDR
Initiator ID protocol	ICMP6	ICMP6	ICMP6	ICMP6
Initiator Identification Data	MN Home Address	MN Home Address	MN Home Address	MN Home Address
Responder ID Type	ID_IPV6_ADDR	ID_IPV6_ADDR	ID_IPV6_ADDR	ID_IPV6_ADDR
Responder ID protocol	ICMP6	ICMP6	ICMP6	ICMP6
Responder Identification Data	HA Address	HA Address	HA Address	HA Address

* w/o Perfect Forward Secrecy (PFS) in IKE Phase 2

** HMAC-SHA1-96 and 3DES-CBC must be selected as Authentication algorithm and Encryption algorithm in "Interoperability test scenario for IPv6 Ready Logo Phase 2 program"

4.4.5. Payload [Tunnel Mode]

This configuration is for development. It is not used in "Interoperability test scenario for IPv6 Ready Logo Phase 2 program".

<SPD for HA (inbound) and MN (outbound) (refer to 1 and 4 in Figure 4.2)>

Source Address	MN Home Address
Destination Address	Any
IPsec Protocol	ESP
Transport Layer Protocol	Any
IPsec protocol mode	tunnel mode

<SPD for HA (outbound) and MN (inbound) (refer to 2 and 5 in Figure 4.2)>

Source Address	Any
Destination Address	MN Home Address
IPsec Protocol	ESP

Transport Layer Protocol	Any
IPsec protocol mode	tunnel mode

<IKE phase2 for MN and HA (refer to 3 and 6 in Figure 4.2)>

	MN0	HA0	MN1	HA2
IPsec Protocol	ESP	ESP	ESP	ESP
Encryption algorithm	3DES-CBC	3DES-CBC	3DES-CBC	3DES-CBC
Authentication algorithm	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96	HMAC-SHA1-96
Life Type	Second	Second	Second	Second
Life Duration	840	840	840	840
Encapsulation Mode	tunnel mode	tunnel mode	tunnel mode	tunnel mode
Initiator ID Type	ID_IPV6_ADDR	ID_IPV6_ADDR	ID_IPV6_ADDR	ID_IPV6_ADDR
Initiator ID protocol	0 (Any)	0 (Any)	0 (Any)	0 (Any)
Initiator Identification Data	MN Home Address	MN Home Address	MN Home Address	MN Home Address
Responder ID Type	ID_IPV6_ADDR _SUBNET	ID_IPV6_ADDR _SUBNET	ID_IPV6_ADDR _SUBNET	ID_IPV6_ADDR _SUBNET
Responder ID protocol	0 (Any)	0 (Any)	0 (Any)	0 (Any)
Responder Identification Data	0 (Any)	0 (Any)	0 (Any)	0 (Any)

* w/o Perfect Forward Secrecy (PFS) in IKE Phase 2

** HMAC-SHA1-96 and 3DES-CBC must be selected as Authentication algorithm and Encryption algorithm in “Interoperability test scenario for IPv6 Ready Logo Phase 2 program”

****

This documentation is produced by Mobile IPv6 SWG members of Certification WG in the IPv6 Promotion Council.

The SWG members currently include Nippon Telegraph and Telephone Corporation (NTT), Yokogawa Electric Corporation, YASKAWA INFORMATION SYSTEMS Corporation, and NTT Advanced Technology Corporation (NTT-AT).

AUTHOR'S LIST

Yasushi Takagi (NTT)

Masaya Tanaka (NTT)

Masaharu Sasaki (NTT)

Keisuke Sakitani (NTT)

Masamitsu Yoshida (NTT)

Harutaka Ueno (NTT)

Takaaki Sato (NTT)

Hiroshi Miyata (Yokogawa Electric Corporation)

Yukiyo Akisada (Yokogawa Electric Corporation)

Kaoru Inoue (YASKAWA INFORMATION SYSTEMS Corporation)

Mitsuharu Okumura (YASKAWA INFORMATION SYSTEMS Corporation)

Kiyoaki Kawaguchi (YASKAWA INFORMATION SYSTEMS Corporation)

Minako Araki (YASKAWA INFORMATION SYSTEMS Corporation)

Kouichiro Ohgushi (YASKAWA INFORMATION SYSTEMS Corporation)

Tamami Miyazaki (YASKAWA INFORMATION SYSTEMS Corporation)

Shiho Homan (YASKAWA INFORMATION SYSTEMS Corporation)

Yoshio Yoshida (NTT-AT)

Noriko Mizusawa (NTT-AT)

Taisuke Sako (NTT-AT)